การรักษาความมั่นคงปลอดภัย ระบบสารสนเทศของ ทร.

สโมสรสัญญาบัตร ฐท.สส.

๑๖ มิ.ย.๕๙ ๐๙๐๐-๑๒๐๐

น.ท.ดร.ณัฐพนธ์ ชาติปรีชากุล
หน.รักษาความมั่นคงปลอดภัย กองสงครามไซเบอร์
สำนักปฏิบัติการ สสท.ทร.

ประวัติการศึกษา

- นักเรียนเตรียมทหาร รุ่นที่ ๓๗
- นักเรียนนายเรือ รุ่นที่ ๙๔
- นักเรียนนายเรืออังกฤษ (Britannia Royal Naval College)
- ปริญญาตรี Electronic System Engineering, Cranfield University
- ปริญญาโท-เอก “Wireless Computer Network Security” Cranfield University
- หลักสูตรนายทหารพรรคนาวิน รุ่นที่ ๕๔
- หลักสูตรเสนาธิการทหารเรือ รุ่นที่ ๗๓

ประวัติการรับราชการ

- ประจำ กร.
- ประจำแผนกสื่อสารสากล กนผ.สส.ทร.
- นคข.ศกส.สส.ทร. และ ธง จก.สส.ทร.
- ประจำแผนกตรวจสอบความพร้อมเพรียง กอส.สส.ทร.
- นายทหารสงครามสารสนเทศ แผนกปฏิบัติการสงครามสารสนเทศ กปท.สสท.ทร.
- หน.ปฏิบัติการสงครามสารสนเทศ กปท.สสท.ทร.
- หน.รักษาความมั่นคงปลอดภัย กสซ.สปก.สสท.ทร.

หัวข้อการบรรยาย

- การรักษาความปลอดภัยระบบสารสนเทศของ ทร.
  - ภัยคุกคามระบบสารสนเทศ
  - แนวความคิดการรักษาความมั่นคงปลอดภัยแบบ Defense in Depth
  - การดำเนินการเกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศของกองทัพเรือ
  - ระเบียบ และแนวทางที่เกี่ยวข้อง
  - สาธิตการ Hack (หากมีเวลาเพียงพอ)
- ประชาสัมพันธ์การแข่งขัน Navy Cyber Contest 2559

การรักษาความปลอดภัยระบบสารสนเทศ

ภัยคุกคามระบบสารสนเทศ ๑

Cyber Threats

สถิติภัยคุกคามสารสนเทศ (55 - 59)

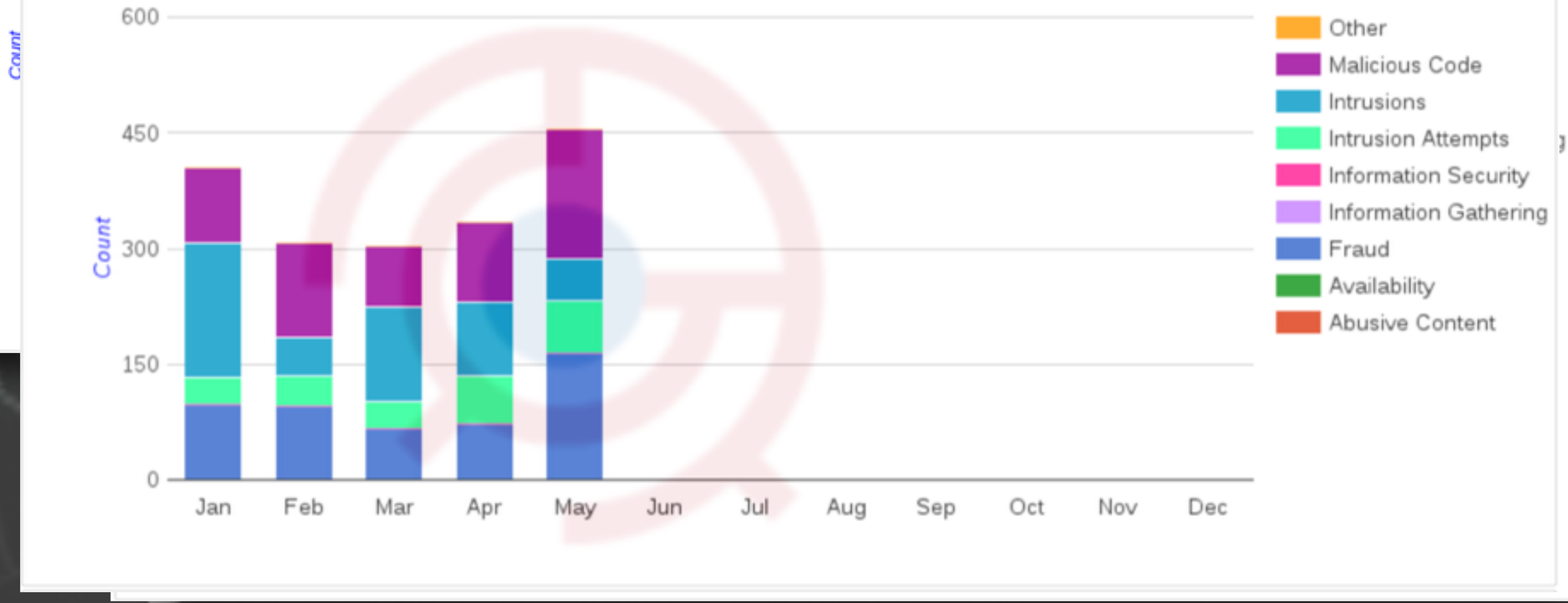
สถิติภัยคุกคาม ประจำปี พ.ศ. 2555

จำแนกเป็นรายเดือน

สถิติภัยคุกคาม ประจำปี พ.ศ. 2558

สถิติภัยคุกคาม ประจำปี พ.ศ. 2559

จำแนกเป็นรายเดือน



ที่มา: ThaiCERT.or.th

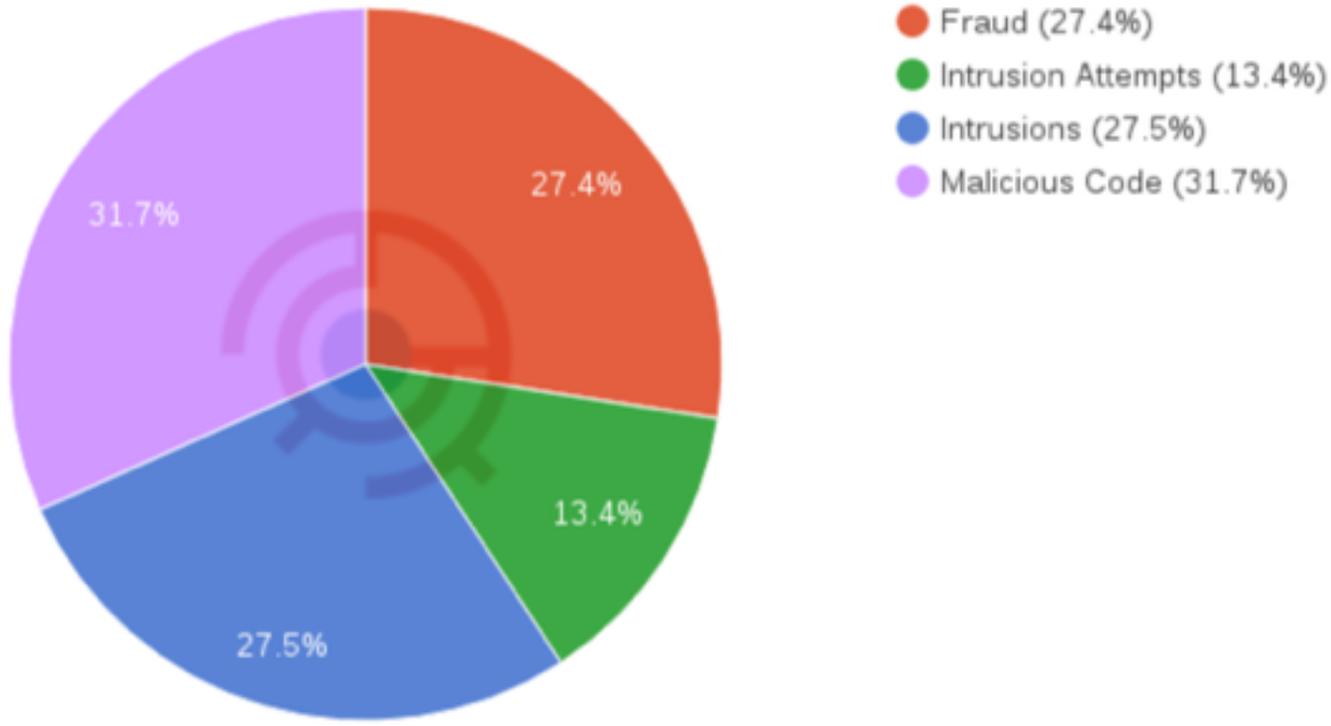
สถิติภัยคุกคามสารสนเทศ

สถิติภัยคุกคาม ประจำปี พ.ศ. 2558

สถิติภัยคุกคาม ประจำปี พ.ศ. 2559

จำแนกเป็นรายเดือน

จำแนกตามประเภทภัยคุกคาม



ที่มา: ThaiCERT.or.th

ตัวอย่างภัยคุกคามสารสนเทศ

- ประเภทหลอกลวง (Fraud/Phishing)
  - แก๊ง call center หลอกโอนเงิน ATM
  - หลอกให้เปลี่ยนรหัสบัญชี online banking
- Phishing อื่นๆ

แก๊ง Call Center

Phishing

ภัยทุจริตทางอินเทอร์เน็ตประเภท Phishing

Phishing คือ วิธีที่กลุ่มมิจฉาชีพใช้ในการโจรกรรมข้อมูล อาศัยรูปแบบของการปลอมแปลงอีเมล์ แอบอ้างมาจากสถาบันการเงิน และแนบ **link สร้างเว็บไซท์ปลอม**ที่เลียนแบบให้คล้ายคลึงกับเว็บไซท์จริง มุ่งหลอกลวงให้ผู้รับอีเมล์เข้าใจผิด หลงเชื่อเปิดเผยข้อมูลส่วนตัวทางด้านการเงิน หรือข้อมูลสำคัญอื่นๆ เช่น ข้อมูลบัตรเครดิต บัญชีผู้ใช้บริการและรหัสผ่าน ข้อมูลรหัสบัตรเอทีเอ็ม ข้อมูลบัตรประจำตัวประชาชน หมายเลขประกันสังคม และอื่นๆ เพื่อกลุ่มมิจฉาชีพจะได้สามารถนำข้อมูลนั้นไปกระทำการทุจริตฉ้อโกงต่างๆ

ส่วนใหญ่ **Phishing** จะใช้กลยุทธทางด้านจิตวิทยา โดยสร้างความเชื่อถือและจุดสนใจ หรือประเด็นสำคัญเร่งด่วน อาทิเช่น ส่งอีเมล์แจ้งว่าเป็นเรื่องเร่งด่วนจากธนาคาร แจ้งปิดบัญชีลูกค้า แจ้งเรื่องบัตรเครดิตหมดอายุ แจ้งขอสำรวจข้อมูลลูกค้า การเสนอโปรโมชั่นพิเศษ เพื่อหลอกลวงให้ลูกค้าหลงเชื่อ ป้อนข้อมูลส่วนตัวบนหน้าจอ หรือทำรายการไปยังเว็บไซท์อื่น เป็นต้น

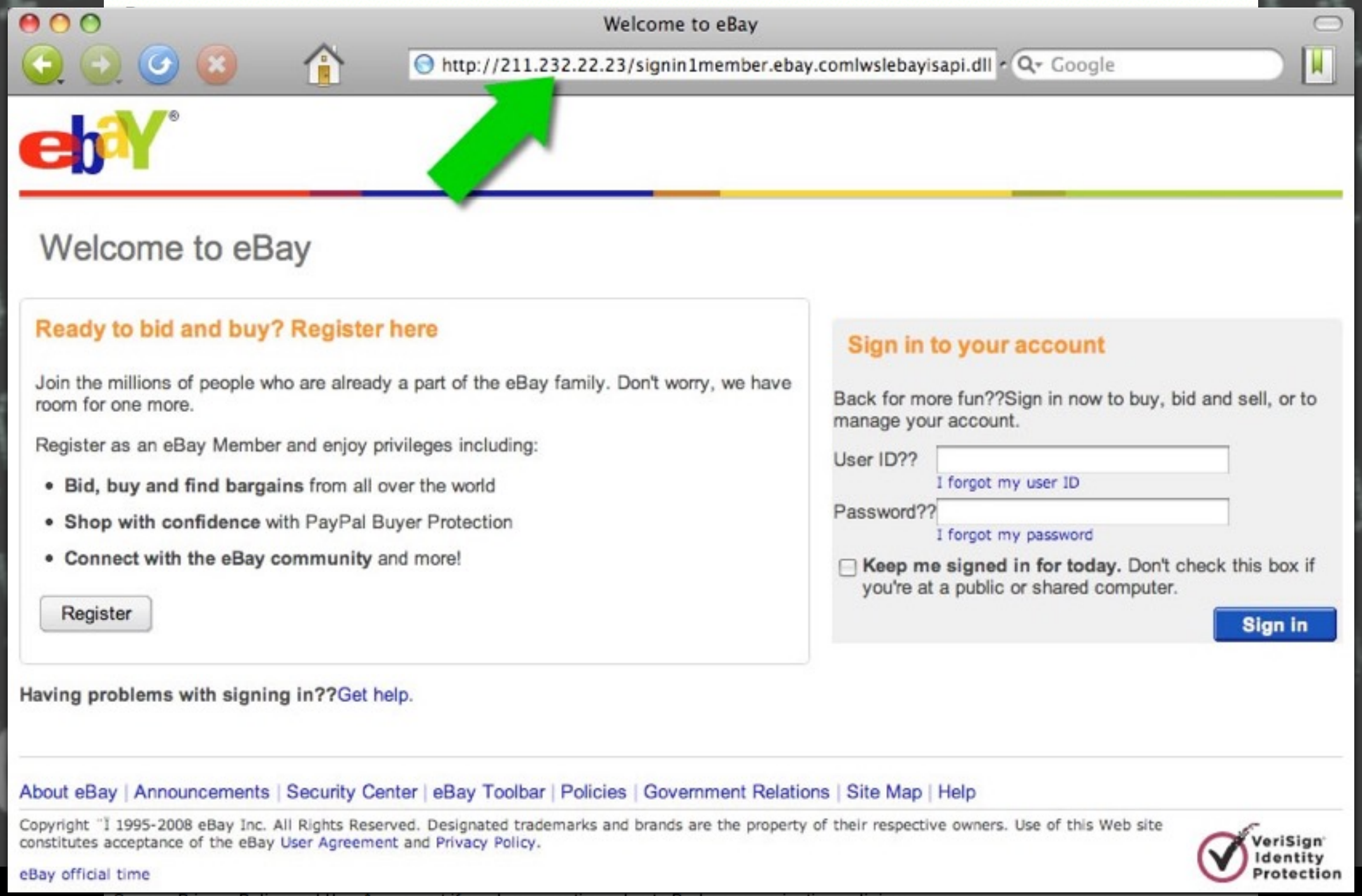
ข้อแนะนำเพื่อการป้องกัน

- ผู้ใช้บริการ ควรดูแลและป้องกันข้อมูลส่วนบุคคลของท่านให้ปลอดภัยที่สุด
- ควรตรวจสอบความถูกต้องของรายการธุรกรรมทางการเงิน และยอดเงินในบัญชีอย่างสม่ำเสมอ เพื่อป้องกันรายการผิดปกติที่อาจเกิดขึ้น
- ถ้าไม่มั่นใจกับอีเมล์ที่ได้รับ หรืออีเมล์ที่มีพฤติกรรมน่าสงสัย ควรยกเลิกลบทิ้ง ไม่ควรป้อนข้อมูล หรือตอบกลับอีเมล์นั้น
- ไม่ควรคลิก Link อำนวยความสะดวกที่แนบมาในเอกสารอิเล็กทรอนิกส์ อนึ่งเพื่อความมั่นใจในการใช้งานอย่างปลอดภัย ควรพิมพ์ address ของเว็บไซท์ที่ท่านสนใจเข้าเยี่ยมชมด้วยตนเองเท่านั้น

หลีกเลี่ยงการรันโปรแกรมที่ส่งมาพร้อมกับอีเมล์ เนื่องจากอาจเป็นโปรแกรมประสงค์ร้ายที่แฝงเข้ามาดักจับข้อมูลส่วนตัวสำคัญของท่าน หรือก่อกวนทำลายระบบข้อมูลในเครื่องคอมพิวเตอร์ของท่านได้

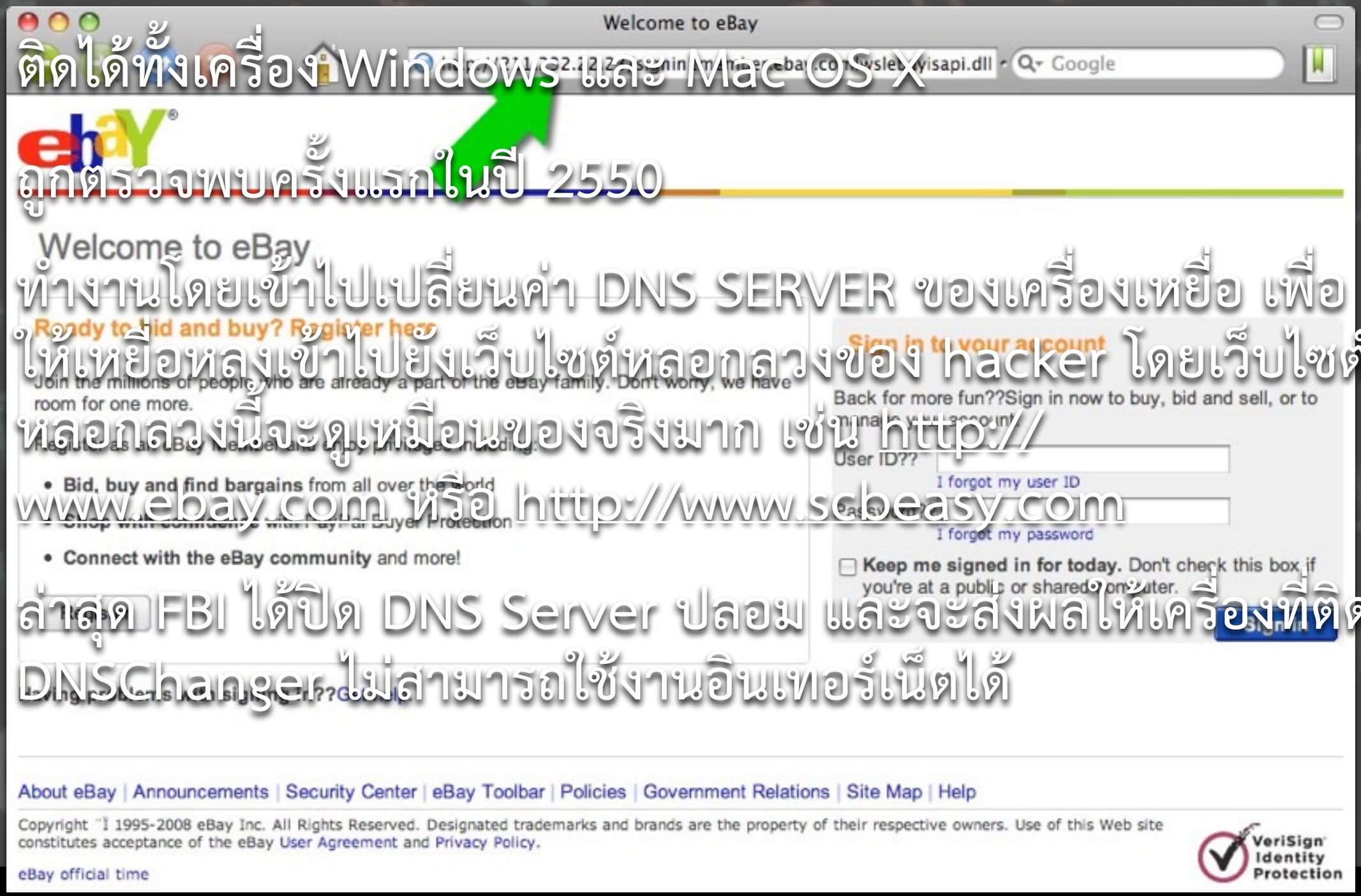
ทั้งนี้ ขอเรียนแจ้งว่าธนาคารไม่มีนโยบายในการสอบถามข้อมูลส่วนบุคคลที่เป็นความลับของลูกค้า เช่น ชื่อบัญชี ผู้ใช้บริการ รหัสผ่าน **Password** รหัสบัตร **ATM** หมายเลขบัญชี หมายเลขบัตรเครดิต หมายเลขบัตรประชาชน ผ่านทางอีเมล์ ผ่านทางโทรศัพท์ หรือผ่านทางข้อความทางโทรศัพท์มือถือ **(SMS)** เป็นต้น

Phishing


Welcome to eBay
http://211.232.22.23/signin1member.ebay.comlwslebayisapi.dll
Google
ebay
Welcome to eBay
Ready to bid and buy? Register here
Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.
Register as an eBay Member and enjoy privileges including:
Bid, buy and find bargains from all over the world
Shop with confidence with PayPal Buyer Protection
Connect with the eBay community and more!
Register
Sign in to your account
Back for more fun??Sign in now to buy, bid and sell, or to manage your account.
User ID??
I forgot my user ID
Password??
I forgot my password
Keep me signed in for today. Don't check this box if you're at a public or shared computer.
Sign in
Having problems with signing in??Get help.
About eBay | Announcements | Security Center | eBay Toolbar | Policies | Government Relations | Site Map | Help
Copyright © 1995-2008 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.
eBay official time
VeriSign Identity Protection
See our Privacy Policy and User Agreement if you have questions about eBay's communication policies.
Privacy Policy: http://pages.ebay.com/help/policies/privacy-policy.html
User Agreement: http://pages.ebay.com/help/policies/user-agreement.html

Phishing: DNSChanger

- ติดได้ทั้งเครื่อง Windows และ Mac OS X
- ถูกตรวจพบครั้งแรกในปี 2550
- ทำงานโดยเข้าไปเปลี่ยนค่า DNS SERVER ของเครื่องเหยื่อ เพื่อให้เหยื่อหลงเข้าไปยังเว็บไซต์หลอกลวงของ hacker โดยเว็บไซต์หลอกลวงนี้จะดูเหมือนของจริงมาก เช่น http://www.ebay.com หรือ http://www.scbeasy.com
- ล่าสุด FBI ได้ปิด DNS Server ปลอม และจะส่งผลให้เครื่องที่ติด DNSChanger ไม่สามารถใช้งานอินเทอร์เน็ตได้

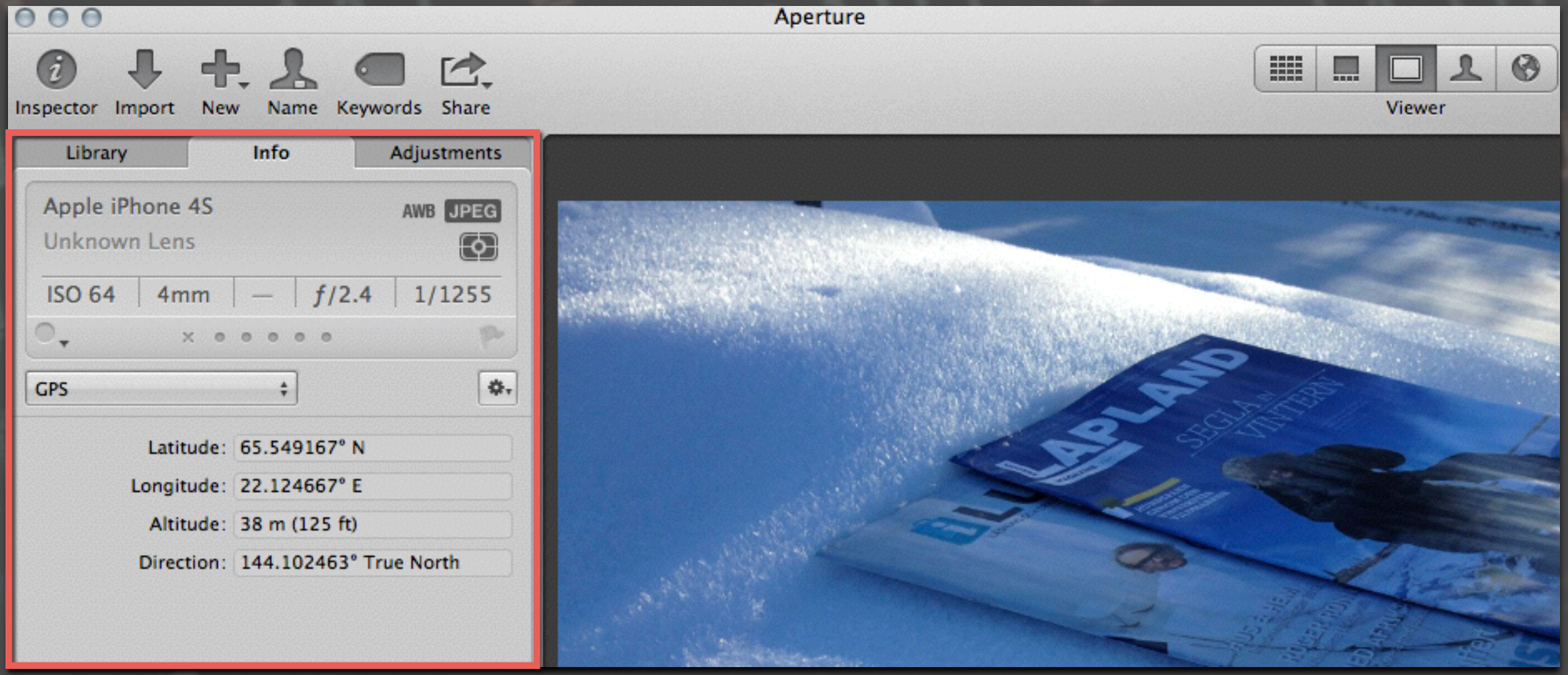


การหาข้อมูลเพื่อทำ Social Engineering

- ปัจจุบันมีการใช้งาน social network หรือเครือข่ายสังคมออนไลน์มาขึ้น ซึ่งเราอาจจะเผลอ post:
  - ข้อมูลสำคัญ หรือมีชั้นความลับ
  - ข้อมูลที่คิดว่าไม่สำคัญเช่น ที่อยู่ วันเดือนปีเกิด รายละเอียดครอบครัว สถานที่อยู่ปัจจุบัน
  - ข้อมูลเหล่านี้หากนำมารวมกัน แฮกเกอร์อาจจะสามารถปลอมเป็นเหยื่อได้

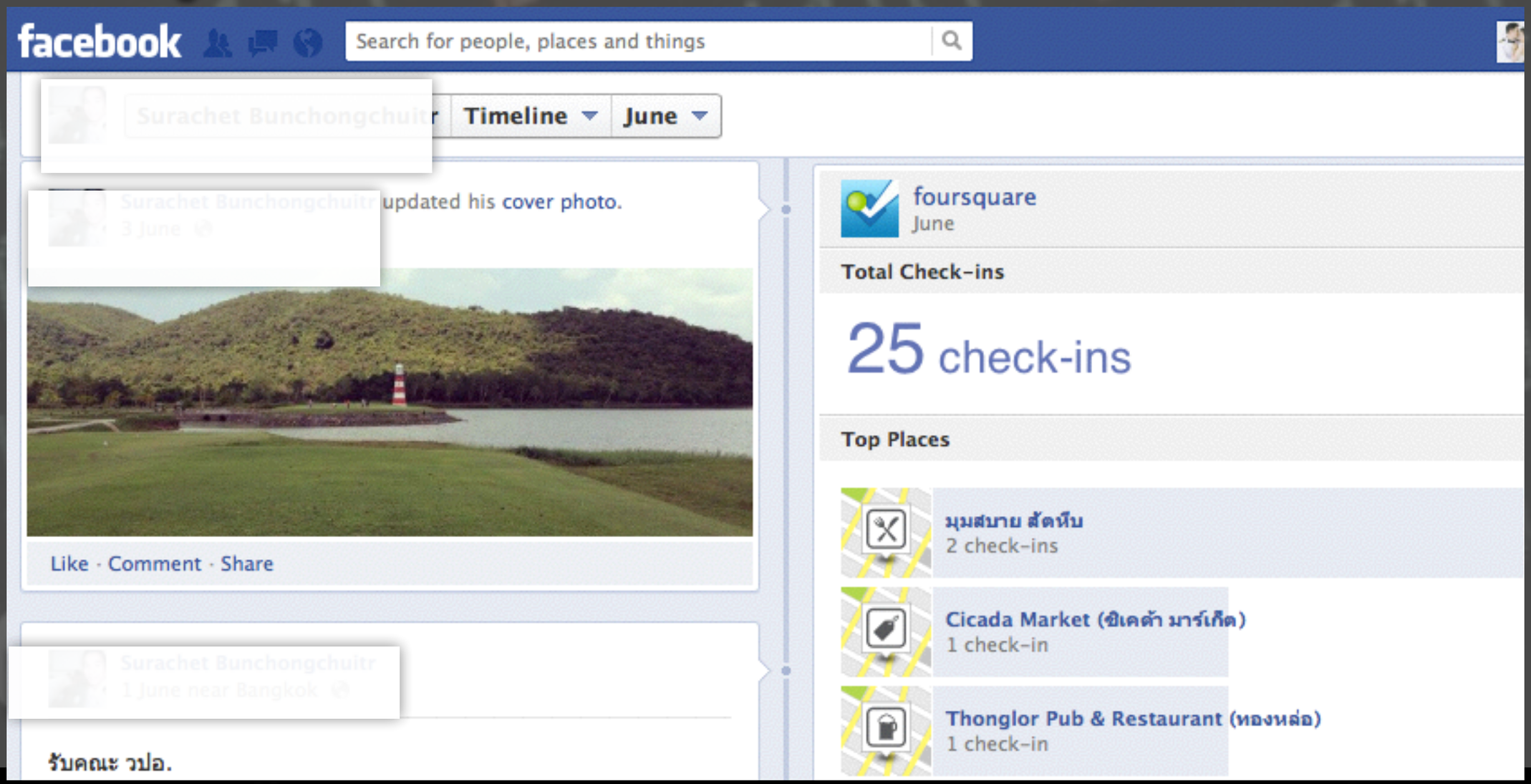
การหาข้อมูลเพื่อทำ Social Engineering

- โทรศัพท์ปัจจุบันมี GPS เมื่อถ่ายรูปจะมีการ tag GPS location ลงไปในภาพ



การหาข้อมูลเพื่อทำ Social Engineering

- การ post ข้อความ/รูป จาก smartphone อาจจะมีข้อมูล location ติดไปด้วย



การหาข้อมูลเพื่อทำ Social Engineering

- ข้อมูลเหล่านี้หากนำมารวมกัน แฮกเกอร์อาจจะสามารถปลอมเป็นเหยื่อได้ เช่น
  - 1ต.ค.54 น.ต. ก.ฯ โพสว่า รับตำแหน่งใหม่เป็น ผบ.เรือ ต.99
  - 5ธ.ค.54 น.ต. ก.ฯ check-in ผ่านมือถือที่ อ.หัวหิน

การหาข้อมูลเพื่อทำ Social Engineering

- ข้อมูลเหล่านี้หากนำมารวมกัน แฮกเกอร์อาจจะสามารถปลอมเป็นเหยื่อได้ เช่น
  - 1ต.ค.54 น.ต. ก.ฯ โพสว่า รับตำแหน่งใหม่เป็น ผบ.เรือ ต.99
  - 5ธ.ค.54 น.ต. ก.ฯ check-in ผ่านมือถือที่ อ.หัวหิน
  - เราสามารถนำข้อมูลทั้งสองชิ้นมารวมกัน ทำให้ทราบได้ว่า ตอนนี้ เรือ ต.99 น่าจะอยู่ที่ หัวหิน

การหาข้อมูลเพื่อทำ Social Engineering

- ตัวอย่างที่ 2
  - นาย เอ check-in ที่บ้าน ย่านบางกะปิ พร้อม GPS coordination
  - นาย เอ โพสข้อความว่า “ไปเที่ยวต่างประเทศพร้อมครอบครัวสองอาทิตย์”
  - ผู้ไม่หวังดีจะทราบจากข้อมูลว่า บ้านนายเอ ไม่มีคนอยู่สองอาทิตย์ เหมาะกับการเข้าไปขโมยของ

มัลแวร์ (Malware: **Mal**icious Soft**ware**)

- มัลแวร์ หมายถึงซอฟท์แวร์ที่ไม่ประสงค์ดี และเป็นภัยต่อระบบสารสนเทศ ข้อมูลที่อยู่ในระบบ
  - ไวรัส
  - หนอนอินเทอร์เน็ต
  - ม้าโทรจัน
  - logic bomb ฯลฯ

Cyber Threats

มัลแวร์: Stuxnet

- Stuxnet เป็นตัวอย่างของการใช้สารสนเทศ (ซอฟท์แวร์ในรูปแบบมัลแวร์) ทำลายขีดความสามารถด้านอื่นที่มิใช่สารสนเทศของฝ่ายตรงข้ามที่ชัดเจนที่สุดในปัจจุบัน
- Stuxnet เป็นหนอนอินเทอร์เน็ตที่ถูกสร้างขึ้น เพื่อใช้ทำลายขีดความสามารถด้านนิวเคลียร์ของอิหร่าน
- จากการวิเคราะห์พบว่า Stuxnet ไม่มีทางที่จะถูกพัฒนาขึ้นโดยไม่ได้รับการสนับสนุนจากภาครัฐ (อาจจะมากกว่า 1 ชาติ ชาติหลัก: อิสราเอล และสหรัฐฯ)

มัลแวร์: Stuxnet

มัลแวร์: Stuxnet

- ระบบที่เป็นเป้าหมายของ Stuxnet คือระบบควบคุมโรงไฟฟ้านิวเคลียร์ของ อิหร่าน ซึ่งเป็นระบบปิด ไม่เชื่อมต่อกับเครือข่ายใดๆ รวมทั้ง Internet (ตัวอย่างของระบบ SCADA: Supervisory Control and Data Acquisition)
- การแพร่ระบาดใช้ช่องโหว่ของระบบปฏิบัติการ Windows ในการแพร่ระบาดผ่านทาง Removable media (thumbdrive) แพร่ระบาดในวง LAN แบบ peer-to-peer แพร่ระบาดผ่านเครือข่ายอินเทอร์เน็ต

มัลแวร์: Stuxnet

- มีระบบการอัพเดต และรายงานผลไปยังผู้สร้างผ่านอินเทอร์เน็ต ผ่านเว็บไซต์ที่จดทะเบียนในมาเลเซีย และ เดนมาร์ก (www.mypremierfutbol.com, www.todaysfutbol.com)
- มีระบบการป้องกันการตรวจจับจากซอฟท์แวร์ป้องกันไวรัส (Kaspersky, McAfee, AntiVir, BitDefender, Etrust, F-Secure, Symantec, Eset NOD32, Trend PC-Cillin)
- มีระบบป้องกันตัวเองแบบ Rootkit (ซ่อนตัวจากการมองเห็นโดยโปรแกรม Windows Explorer)

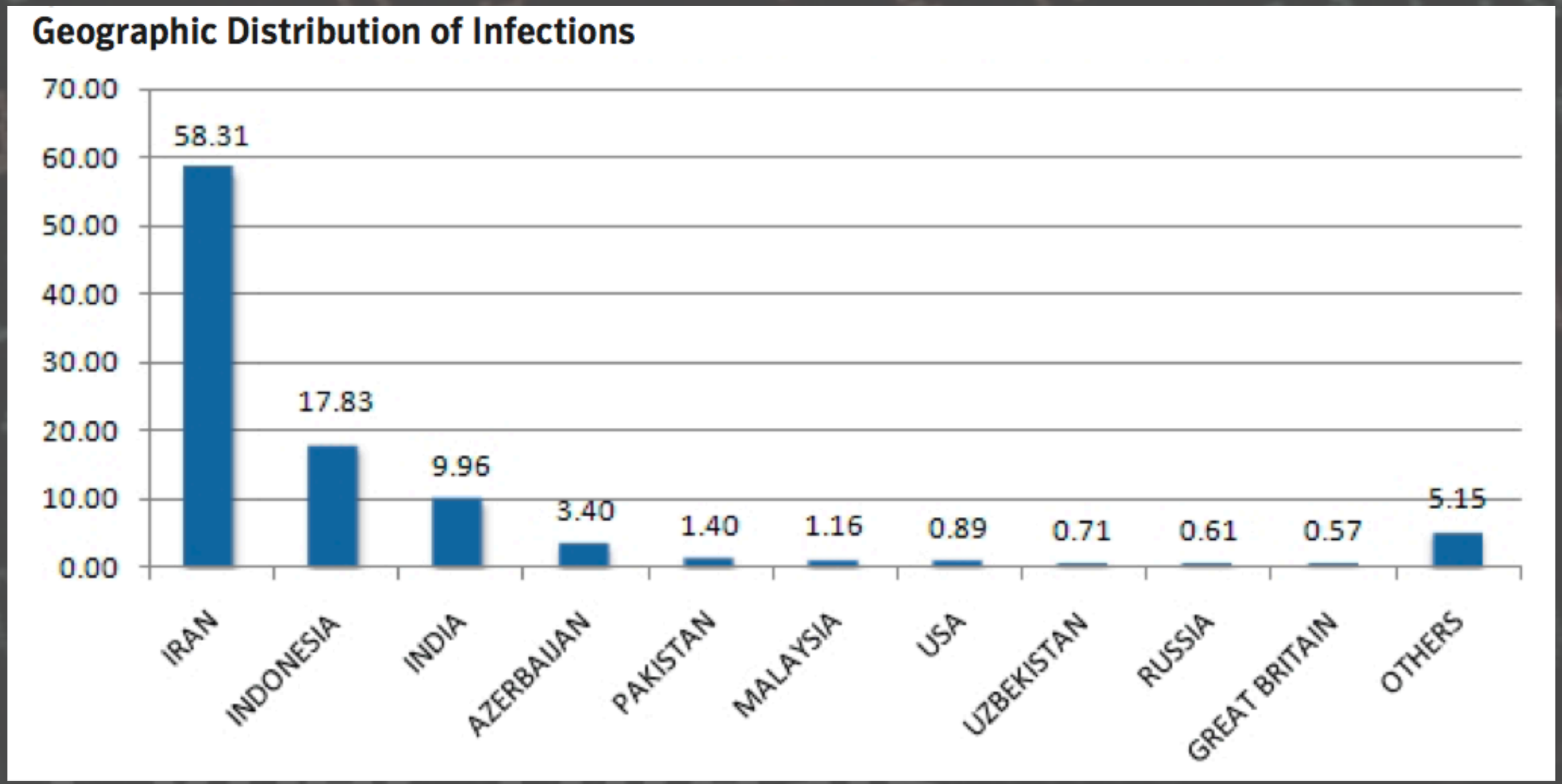
มัลแวร์: Stuxnet

- มีระบบแพร่ระบาดที่ลดโอกาสถูกตรวจจับ โดยจะแพร่ระบาดตัวเองเพียง 3 ครั้งหรือ 3 สัปดาห์หลังจากนั้น ลบตัวเองออก
- การติดตั้งตัวเอง มีการใช้ digital certificate ของแท้ที่ขโมยมาจากบริษัท Jmicron, Realtek
- มีการเก็บราย log ประวัติการแพร่ระบาดตัวเอง โดยจะเก็บ log สถานที่ (เครื่อง) ที่เคยแพร่ระบาด ทำให้ผู้เขียนสามารถตรวจสอบประสิทธิภาพของหนอนดังกล่าวได้

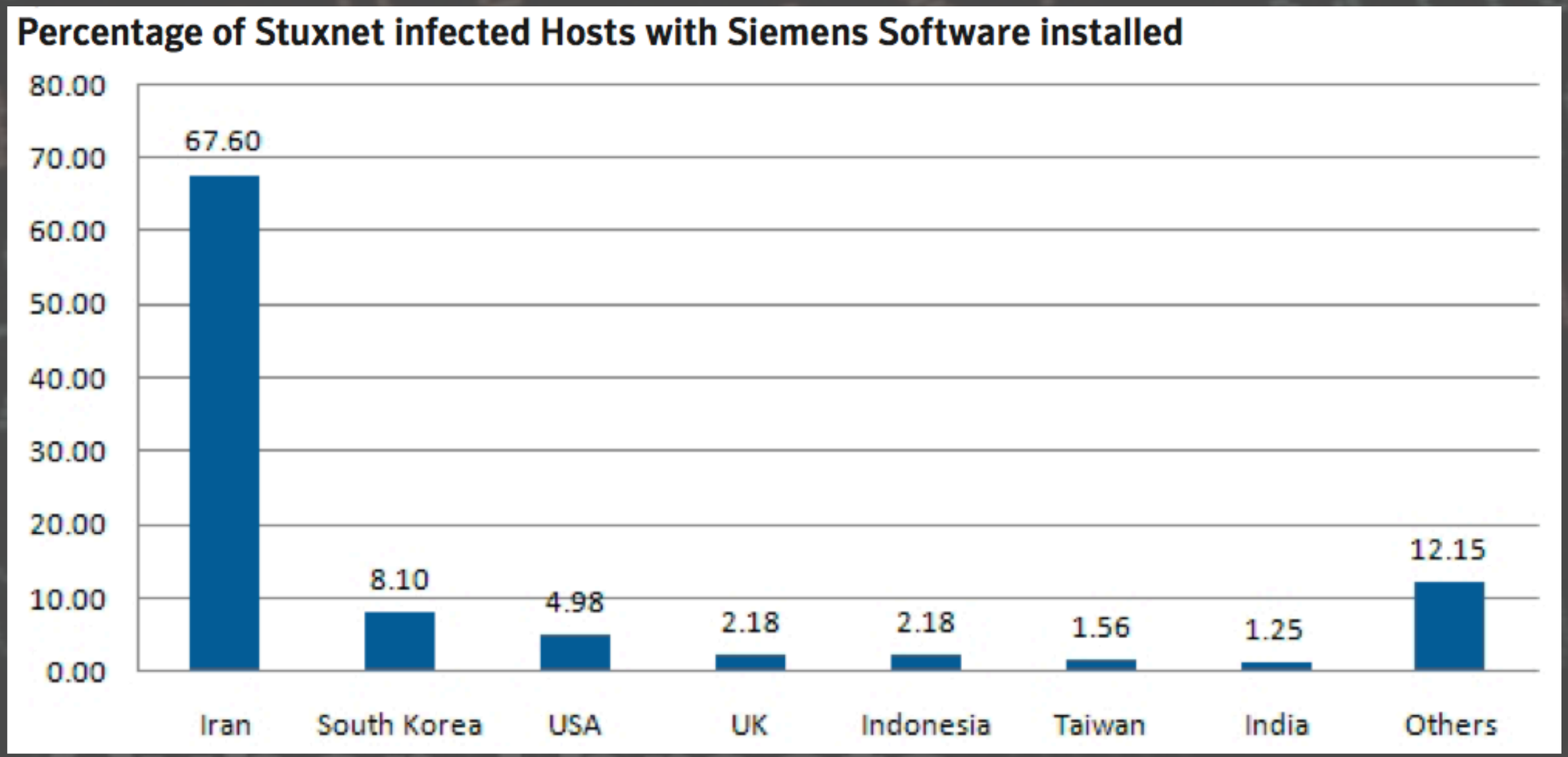
มัลแวร์: Stuxnet

- มีการตรวจสอบเครื่องที่ติด ว่ามีการเชื่อมต่อกับอุปกรณ์ที่ใช้ควบคุมเครื่องจักร (Industrial Control System) ของบริษัท Siemens แบบที่ใช้ในโรงไฟฟ้านิวเคลียร์อิหร่านหรือไม่
- หากสามารถแพร่ระบาดบนเครื่องที่เชื่อมต่อกับระบบ ICS แบบที่ใช้ในโรงไฟฟ้าอิหร่านสำเร็จ จะทำการแก้ไข code มีผลทำให้เครื่องจักรทำการผิดปกติจนเกิดความเสียหายกับแท่งเชื้อเพลิง

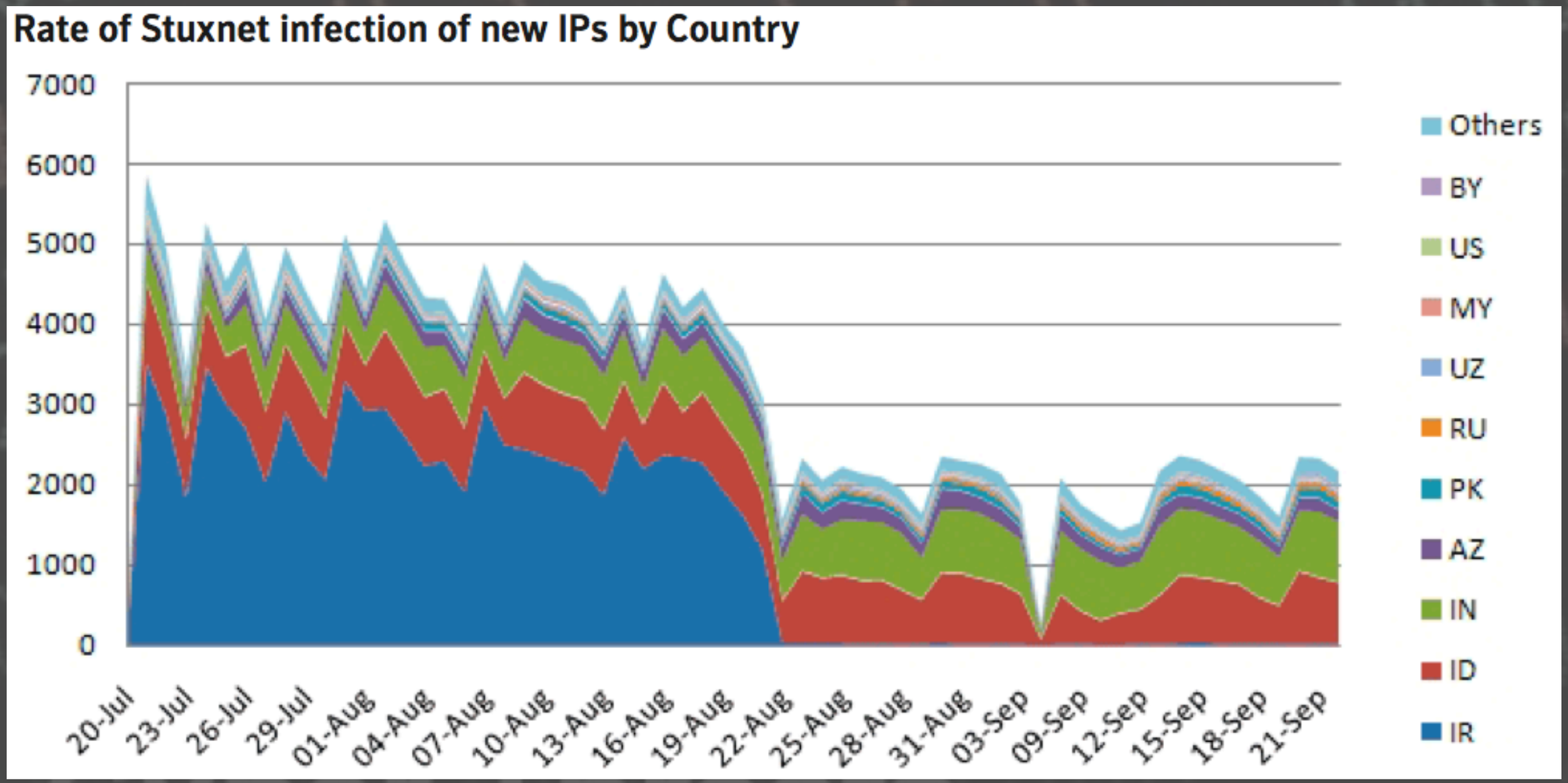
มัลแวร์: Stuxnet



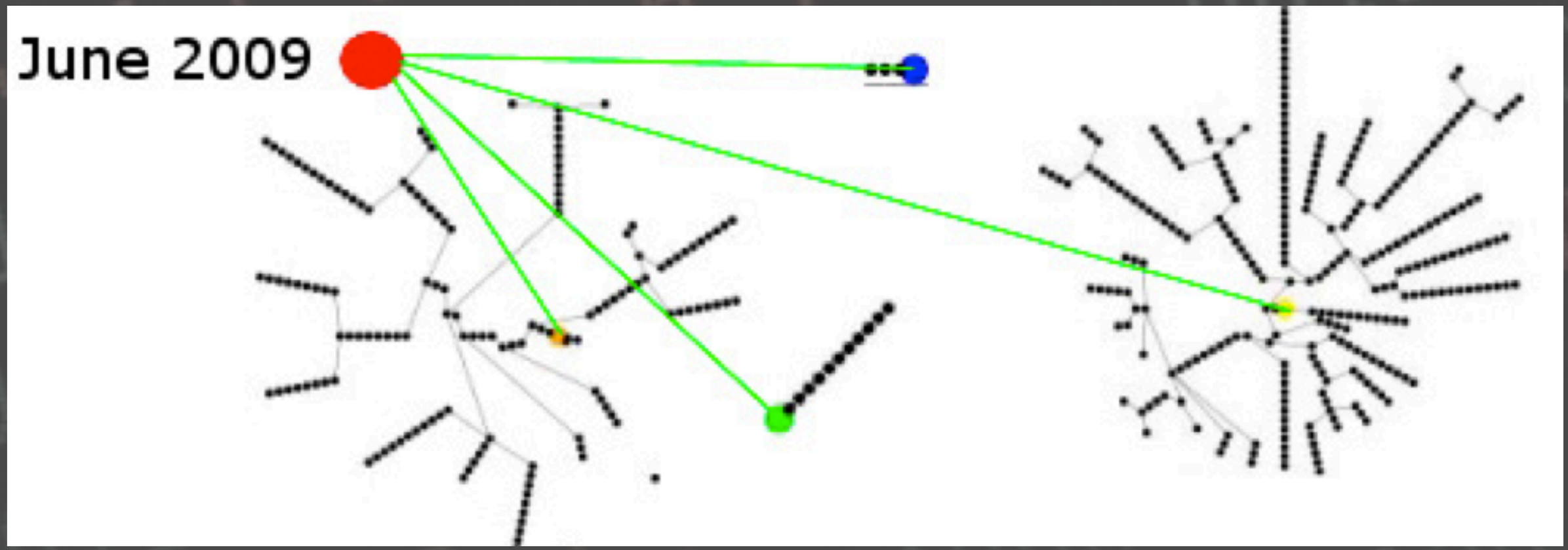
มัลแวร์: Stuxnet



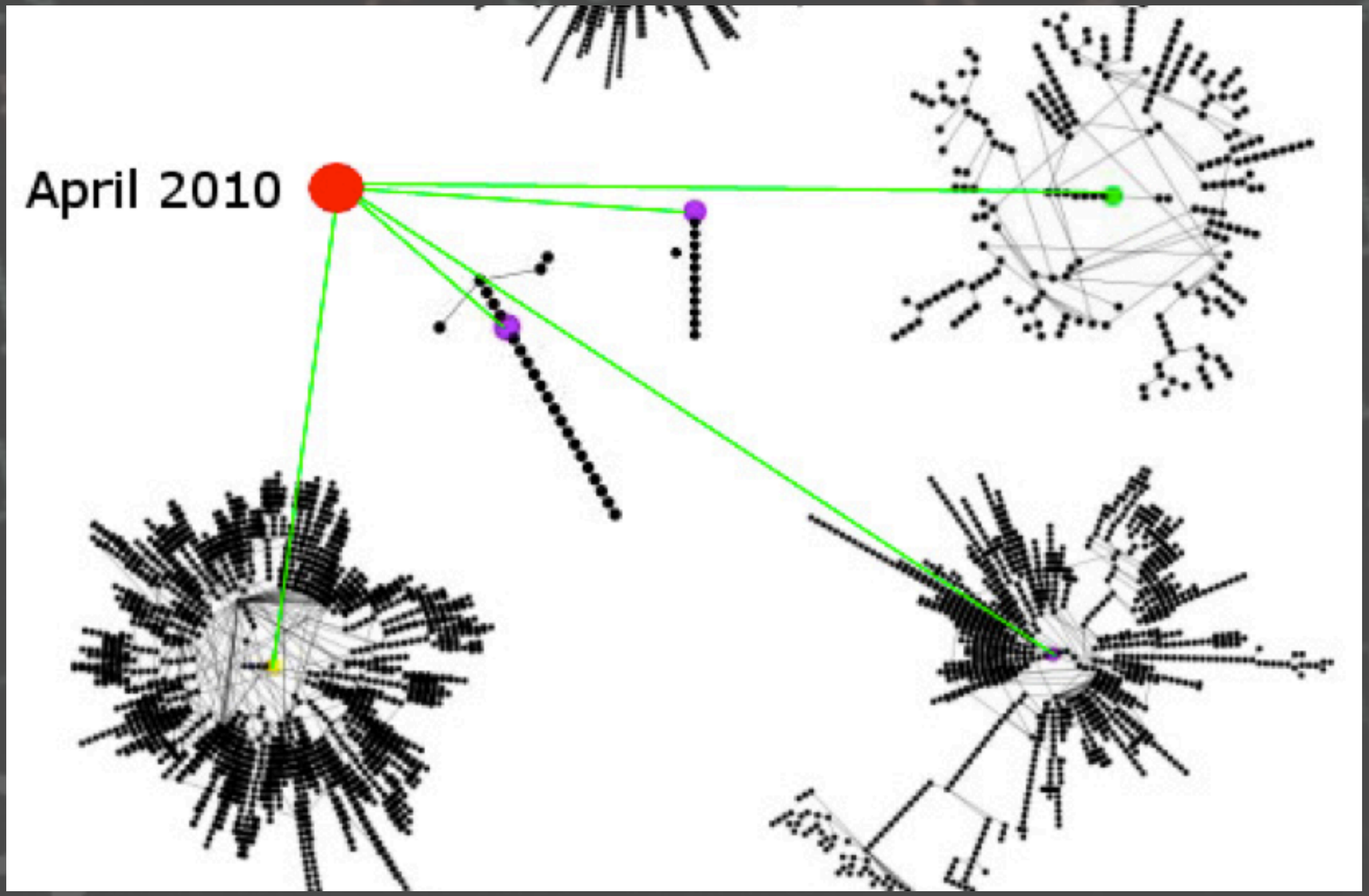
มัลแวร์: Stuxnet



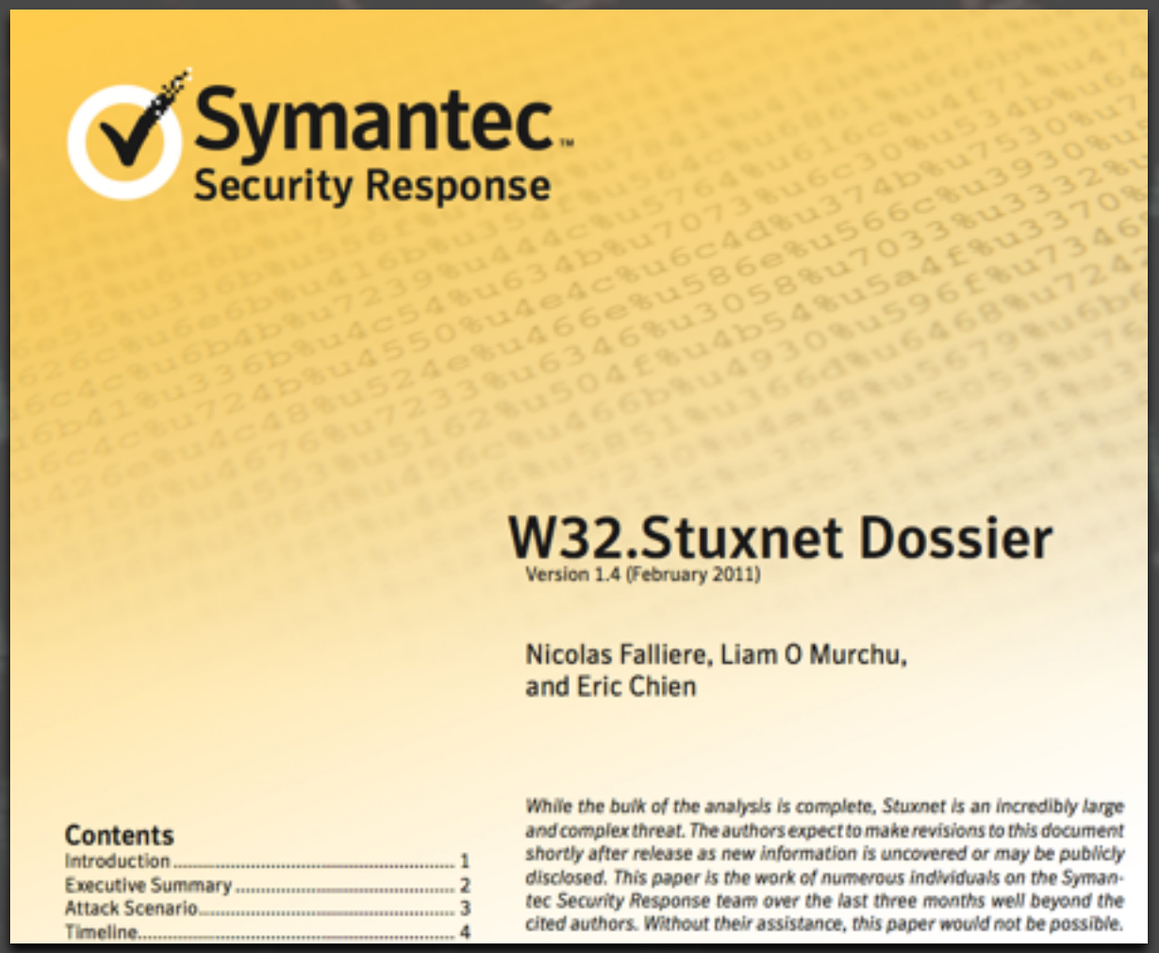
มัลแวร์: Stuxnet



มัลแวร์: Stuxnet



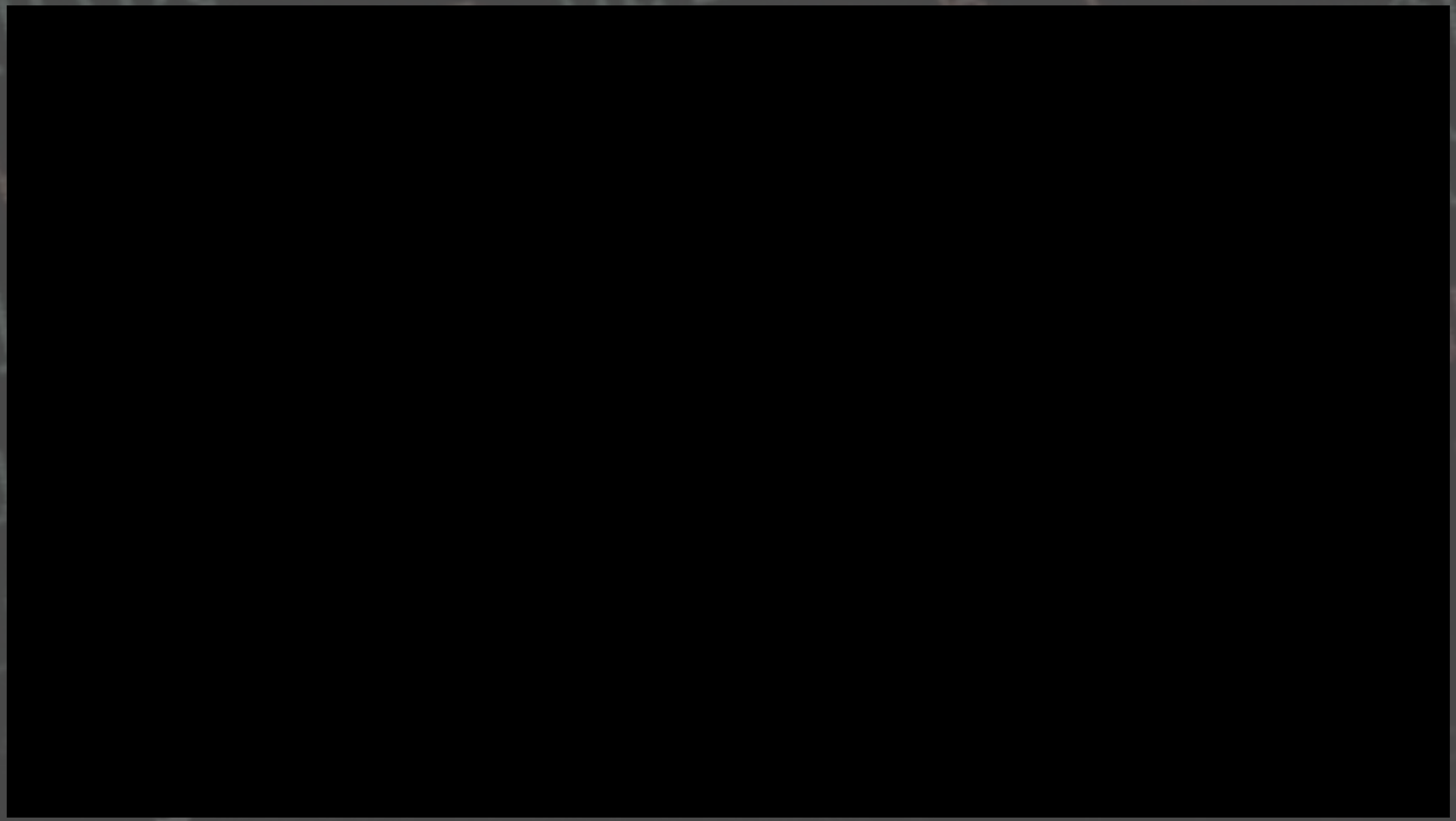
มัลแวร์: Stuxnet



- เอกสารอ้างอิง
  - http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- SecurityNow (episode 291): http://twit.tv/sn291

Cyber Threats

มัลแวร์: Stuxnet



มัลแวร์: Duqu

- ตรวจพบเมื่อปลายปี 2011 (พ.ศ.2553) โดย Laboratory of Cryptography and System Security (CrySyS)
- มีความคล้ายคลึงกับ Stuxnet มากในการทำงาน แต่มีจุดประสงค์ที่ต่างกันโดยสิ้นเชิง
- ได้รับชื่อ Duqu เนื่องจากมันสร้างไฟล์ที่มี ~DQ นำหน้า
- จากการวิเคราะห์พบว่า น่าจะเป็นผู้พัฒนาเดียวกับ Stuxnet หรือสามารถเข้าถึง source code ของ Stuxnet ได้

มัลแวร์: Duqu

- จุดประสงค์หลักของ Duqu คือ เก็บรวบรวมข้อมูล (infostealer) โดยเฉพาะข้อมูลการออกแบบระบบโดยเฉพาะระบบควบคุมเครื่องจักร ซึ่งจะช่วยให้ hacker สามารถออกแบบการโจมตีระบบในอนาคตได้
- แพร่กระจายโดยอาศัยช่องโหว่ของไฟล์ win32k.sys ซึ่งเป็นส่วนที่ใช้สำหรับการแสดงผลตัวอักษรแบบ truetype ของระบบปฏิบัติการ Windows ทุกเวอร์ชั่น
- Duqu หลังจากติดที่เครื่องแล้วจะทำการติดต่อไปยัง C&C ที่อยู่ในประเทศ อินเดีย เบลเยี่ยม และเวียดนาม

มัลแวร์: Duqu

- Duqu ถูกโปรแกรมให้ทำงานบนเครื่องที่ติดเป็นเวลา 30 วัน หลังจากนั้นมันจะลบตัวเองออกจากเครื่อง เพื่อลดโอกาสการถูกตรวจจับ
- ส่วนที่แชร์กันระหว่าง Duqu กับ Stuxnet คือส่วนที่ใช้ในการแพร่กระจาย แต่ส่วน payload คือหลังจากติดแล้วจะทำอะไร จะต่างกันโดยสิ้นเชิง โดย Duqu นั้น payload จะเน้นความสามารถในการให้ hacker เข้าควบคุมเครื่อง (เพื่อใช้เก็บข้อมูล)

มัลแวร์: Flame

- ชื่อที่รู้จัก Flame, Flamer, sKyWiper, Skywiper
- ถูกค้นพบครั้งแรกในปี 2012 โดยหน่วยงานด้านการเฝ้าระวังภัยจากระบบสารสนเทศของประเทศอิหร่าน (MAHER Center of Iranian National Computer Emergency Response Team: CERT)
- มีวัตถุประสงค์เพื่อเก็บและขโมยข้อมูลของหน่วยงานในกลุ่มประเทศตะวันออกกลาง
- จากการวิเคราะห์พบว่ามีการแพร่กระจายก่อน Stuxnet (February 2010)

มัลแวร์: Flame

- การแพร่กระจาย คล้ายกับ Stuxnet และ Duqu คือทั้งผ่านเครือข่ายและอุปกรณ์เก็บข้อมูลแบบพกพา
- ขีดความสามารถ
  - บันทึกเสียงโดยใช้ไมค์โครโฟนที่มากับเครื่อง
  - จับภาพหน้าจอ
  - key logger
  - ดักจับข้อมูลผ่านเครือข่าย
  - บันทึกการสนทนาผ่านโปรแกรม skype
  - ขโมยข้อมูลภายในเครื่อง โดยเน้นเอกสารแบบแปลน PDF และไฟล์เอกสารอื่นๆ

มัลแวร์: Flame

- ขีดความสามารถ (ต่อ)
  - เปิด bluetooth ของเครื่อง พยายามติดต่อกับโทรศัพท์มือถือในบริเวณใกล้เคียงและพยายาม download รายชื่อหมายเลขโทรศัพท์
  - ส่งข้อมูลดังกล่าว พร้อมข้อมูลอื่นๆ ภายในเครื่องที่ติด กลับไปยังหน่วยควบคุม
  - เพิ่มเติมขีดความสามารถใหม่ ผ่านหน่วยควบคุม
- ข้อมูลที่สำคัญ
  - ขนาดของ Flame มีขนาด > 20MB ซึ่งใหญ่มากสำหรับ malware

มัลแวร์: Flame

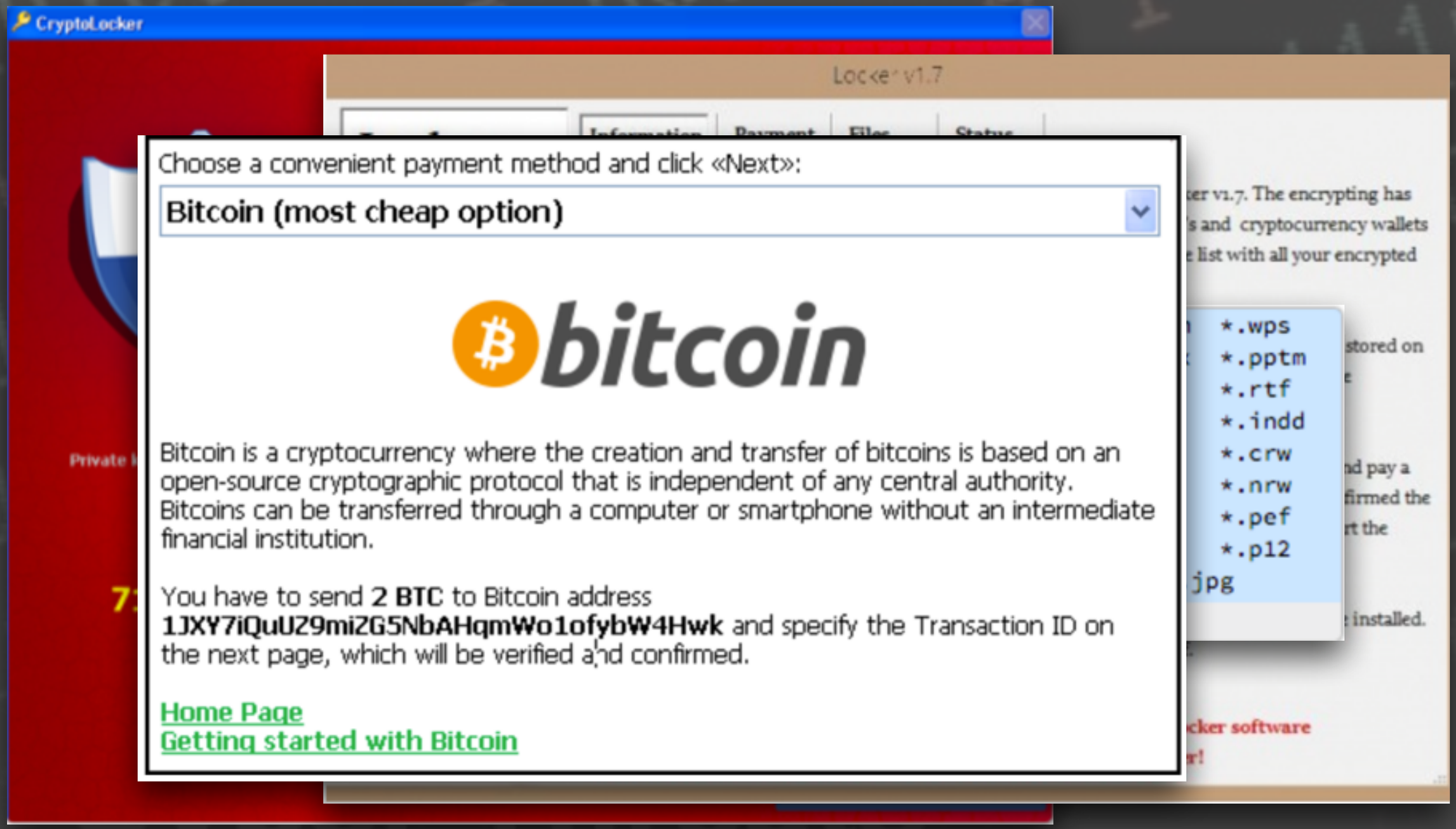
- ข้อมูลที่สำคัญ(ต่อ)
  - ใช้ encryption algorithm ต่างกันถึง 5 แบบ
  - ใช้ SQLite สำหรับเก็บข้อมูล
  - มีระบบหลบหลีกการตรวจจับจากโปรแกรม antivirus
  - ไม่มีระบบทำลายตัวเองเหมือน stuxnet และ duqu แต่สามารถรับคำสั่งให้ลบตัวเองจากหน่วยควบคุม
  - ใช้ช่องโหว่ของการสร้าง certificate จาก service ของ Microsoft Windows เช่น Terminal Server และ WSUS ที่ยังใช้การเข้ารหัสแบบเดิมที่ไม่ปลอดภัย (MD5)

มัลแวร์: Ransomware

- อาศัยช่องโหว่หรือจุดอ่อนของระบบสารสนเทศ เพื่อเข้าควบคุมเครื่องคอมพิวเตอร์
- แทนที่จะทำลายข้อมูล หรือใช้เครื่องฯ เป็นเครื่องมือโจมตีผู้อื่น เปลี่ยนเป็นเข้ารหัสข้อมูลที่คิดว่าสำคัญในเครื่อง แล้วเรียกค่าไถ่ (ransom) โดยให้เหยื่อ จ่ายเงินผ่านช่องทางต่างๆ เช่น bitcoin บัตรเติมเงินต่างๆ

Cyber Threats

มัลแวร์: Ransomware



Insider threat

- ภัยคุกคามจากคนในองค์กร
  - ไม่ควรเข้าถึงแต่มีสิทธิ์เข้าถึง
  - ย้ายออกไปแล้วแต่ยังมีสิทธิ์เข้าถึง
  - ไม่มีกระบวนการควบคุมการเข้าถึง
  - ไม่มีกระบวนการตรวจสอบ
  - ไม่มีกระบวนการสำรองข้อมูล

Cyber Threats

Insider threat

- กรณีศึกษา File server ทรภ.๓*

Share Information

Share name	Confidential Documents	Home Directories Share
Directory to share	/home/Documents	...
Available?	Yes No	
Browseable?	Yes No	
Share Comment		

Save | View Connections | Delete

Directory of /home/

	..	4 kB	11/Dec/2012	00:16
	nattapat	4 kB	21/Aug/2015	10:33

Action	Module	User	Client Address	Date	Time
Ran command ls	Command Shell	admin	10.106.0.1	19/Aug/2015	12:59
Ran command cd nattapat	Command Shell	admin	10.106.0.1	19/Aug/2015	12:59
Ran command ls	Command Shell	admin	10.106.0.1	19/Aug/2015	12:59
Ran command cd /home	Command Shell	admin	10.106.0.1	19/Aug/2015	12:58
Ran command sudo rm -rf /home/*	Command Shell	admin	10.106.0.1	19/Aug/2015	12:58
Ran command sudo rm -rf /home/*	Command Shell	admin	10.106.0.1	19/Aug/2015	12:56
Modified user root	Users and Groups	admin	10.106.0.1	04/Aug/2015	14:38
Modified user root	Users and Groups	admin	10.106.0.1	04/Aug/2015	14:38

Export as CSV.

Return to search form

Insider threat

- กรณีศึกษา File server ทรภ.๓*
  - user ที่มีสิทธิ์ root remote login เข้ามาลบไฟล์
  - มีการเก็บ log
  - ไม่มีการ backup
- ไม่มีการควบคุมสิทธิ์การเข้าถึงของข้าราชการย้ายออก

* ได้รับอนุญาตให้เผยแพร่เป็นกรณีศึกษาจาก ทรภ.๓

Video1


I'm at the station in Utrecht. My mobile
phone has a fast Internet connection.

Video2

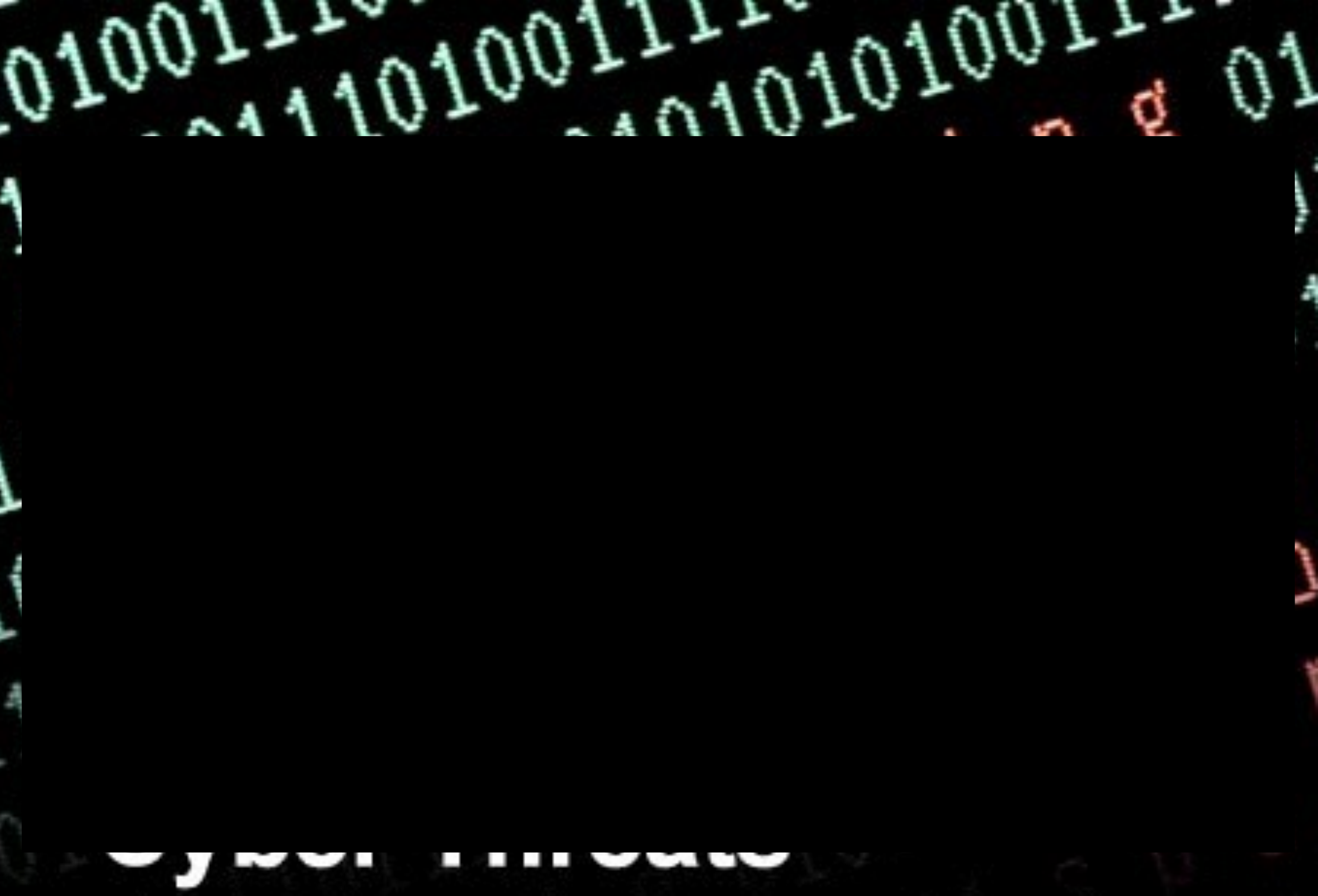

Come see this.

Video3


50
50
50
50

Video4

Cyber Threats


Cyber Threats

Note: video ทั้งหมด มาจาก youtube.com

Cyber Threats

แนวความคิดการรักษาความมั่นคงปลอดภัยแบบเชิงลึก

Defense in Depth

แนวความคิด Defense in Depth

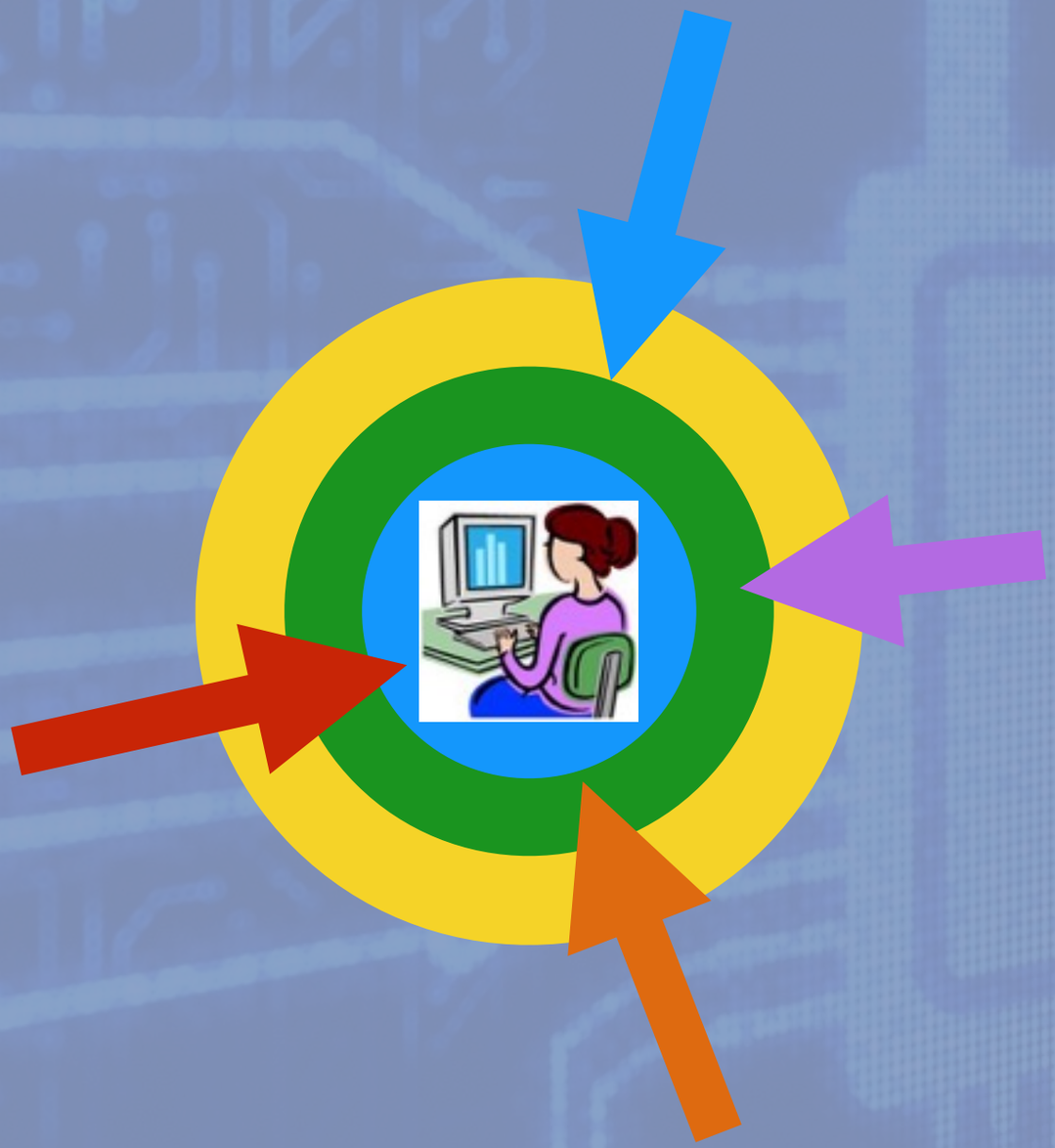
A single security control is never 100% reliable
Attacks may not come from the same attack vector

Should one security layer fail, the remaining layers will prevent severe security compromise from happening

ข้อดีของการดำเนินการ Defense in Depth

- เพิ่มโอกาสที่จะสามารถตรวจจับการโจมตีจากผู้ไม่ประสงค์ดีได้
- ลดโอกาสความสำเร็จของการโจมตีจากผู้ไม่ประสงค์ดี

Defense in Depth: concept to model



Policy, Procedure & Awareness

Physical Security

Perimeter Defense

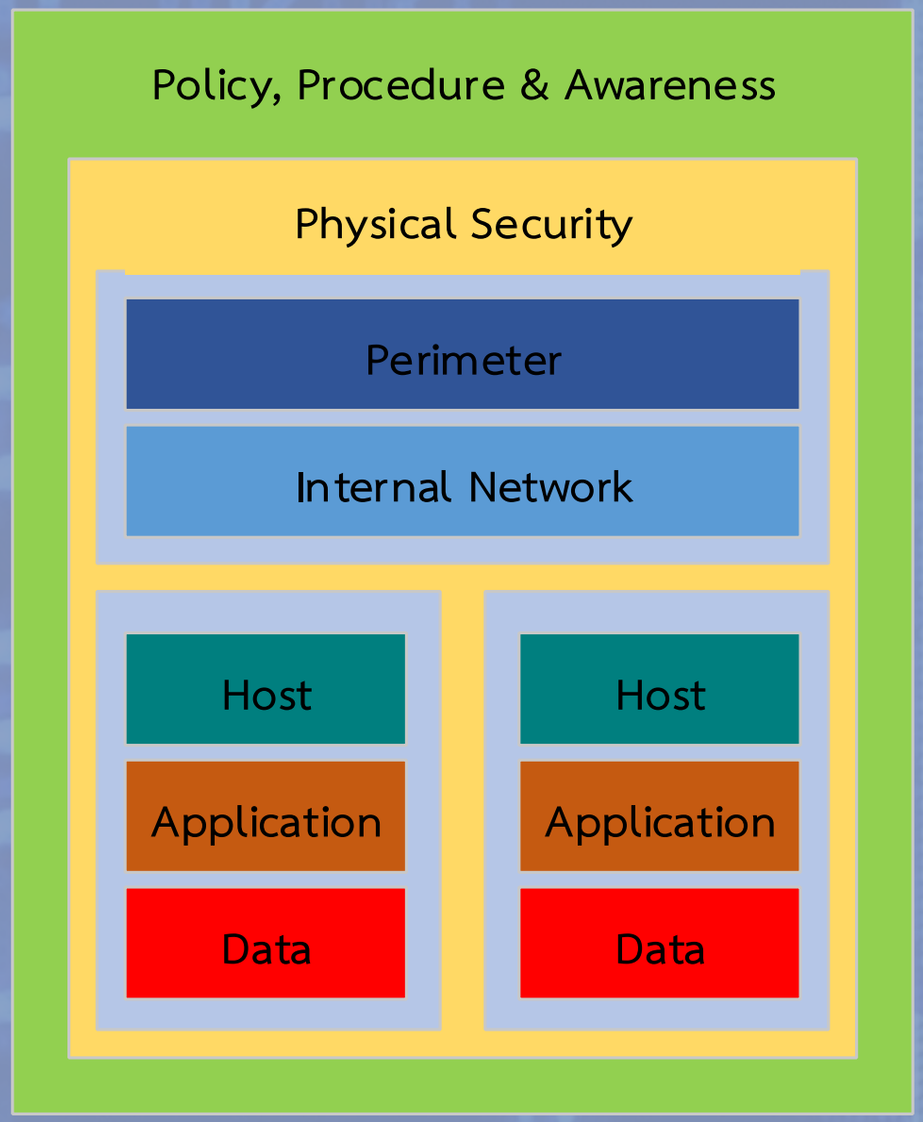
Network Defense

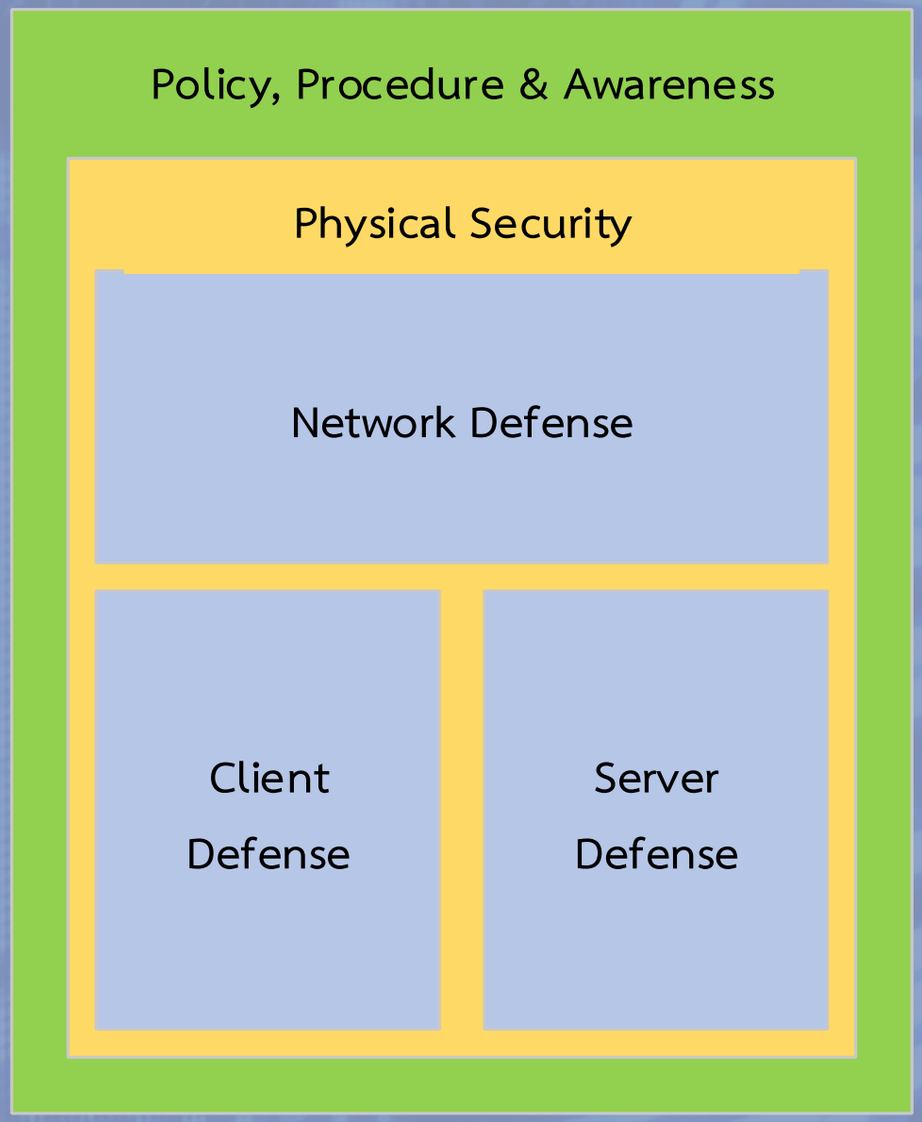
Host Defense

Application Defense

Data Defense

Defense in Depth: concept to model





Network Defense

Internal

Perimeter

Trusted/ Managed

Network

Untrusted/ unmanaged

VPN

Dial-in

LAN/WAN

Internet

Proxy

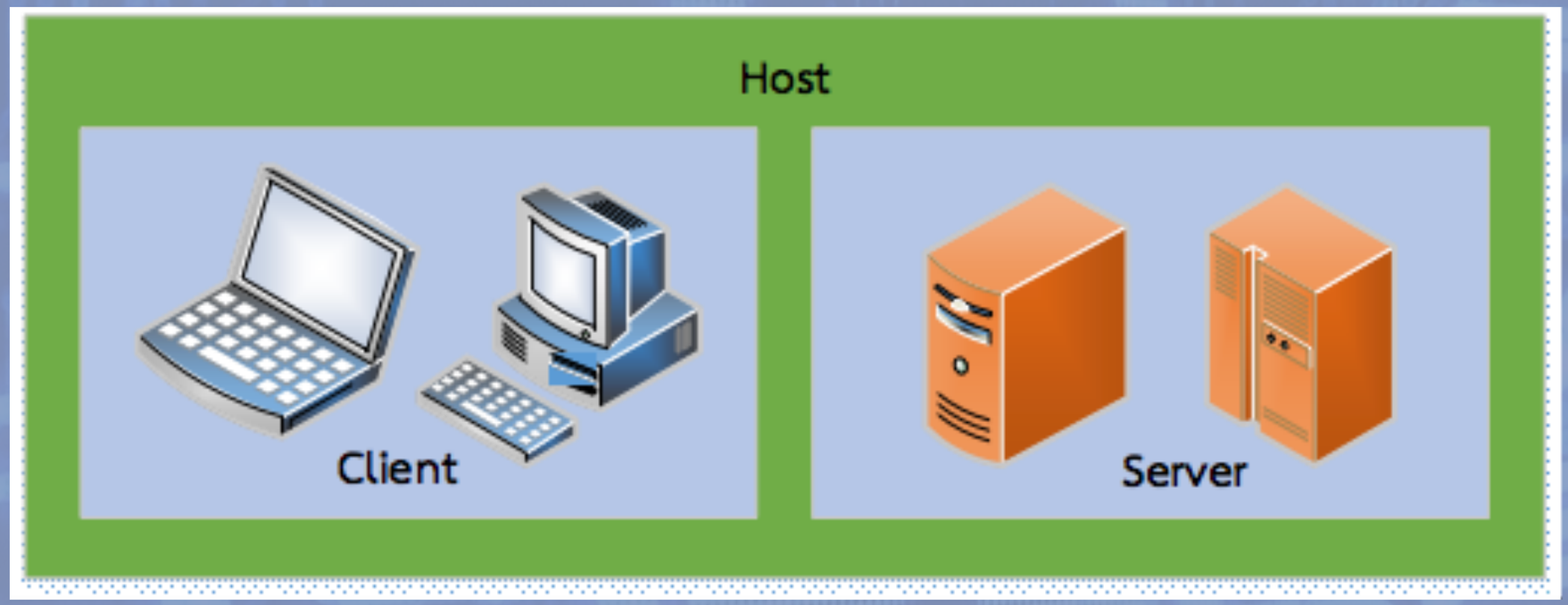
Firewall

IPS/IDS

NAC

Filtering

Host Defense



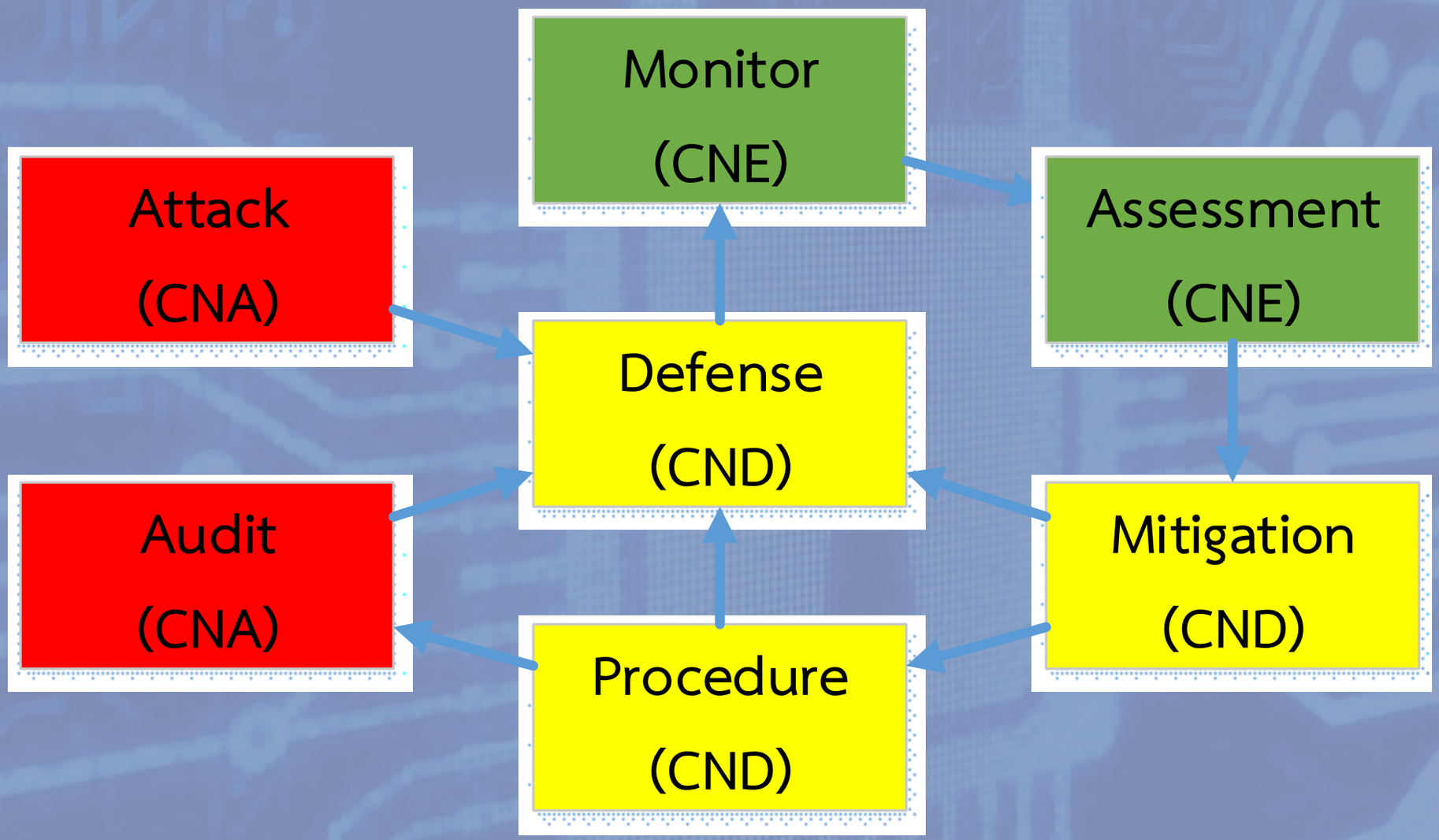
UAC | OS Patch | Endpoint | Firewall | IPS/IDS

Application Defense

- Licensed Software
- Application Patch
- Secured Programming

Data Defense

Cyber Security Framework

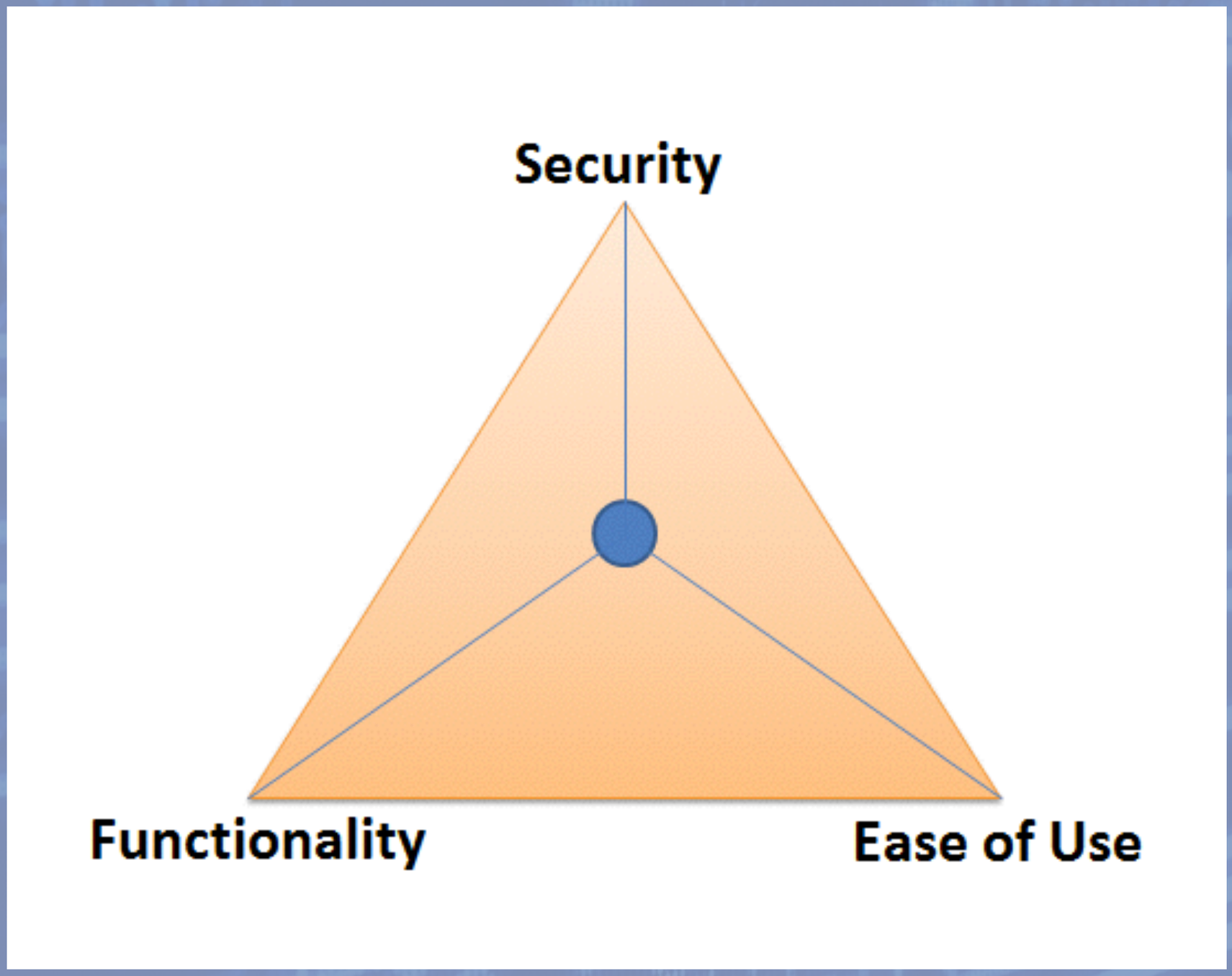


การดำเนินการเกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศของกองทัพเรือ

การ รปภ.ระบบสารสนเทศ อย่างมีประสิทธิภาพ

"การ รปภ. ระบบสารสนเทศ คือการป้องกันระบบสารสนเทศ จากข้อผิดพลาดต่างๆ ทั้งจากการตั้งใจ (intentional) และไม่ตั้งใจ (unintentional)"

อุปสรรคการรักษาความปลอดภัยสารสนเทศ

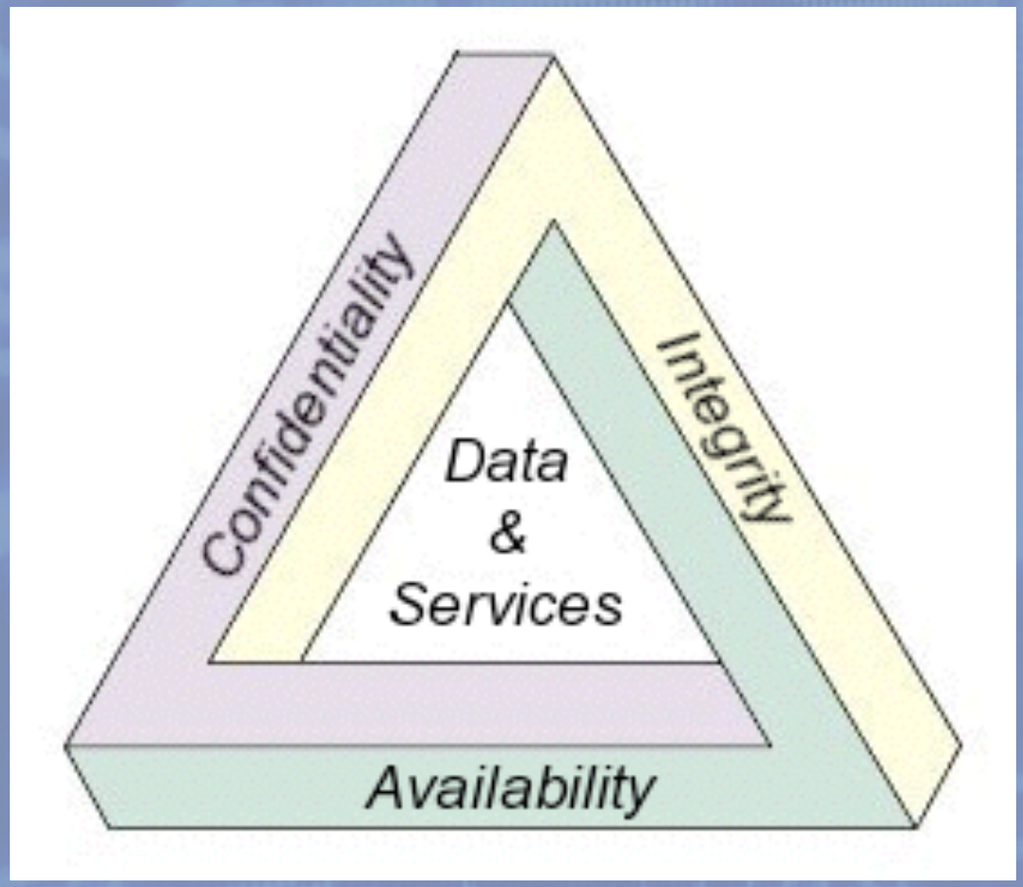


การ รปภ.ระบบสารสนเทศ อย่างมีประสิทธิภาพ

- มีความเข้าใจว่าการรักษาความปลอดภัยระบบสารสนเทศ เป็นกระบวนการ (process) ที่ต้องกระทำอย่างต่อเนื่อง ไม่ใช่เพียงแค่ผลิตภัณฑ์ (product) หรืออุปกรณ์ ซึ่งหาซื้อมาติดตั้งแล้วจะได้ความปลอดภัย
- จัดหาและมีอุปกรณ์หรือผลิตภัณฑ์สำหรับป้องกันและตรวจสอบความปลอดภัยระบบสารสนเทศอย่างเหมาะสม
- สร้างความตระหนักในเรื่องความปลอดภัยให้กับผู้ที่เกี่ยวข้องกับระบบสารสนเทศ ซึ่งไม่ใช่แค่ผู้ดูแลระบบ แต่ยังต้องรวมถึงผู้ใช้งานระบบสารสนเทศด้วย

การได้มาซึ่งความปลอดภัยระบบสารสนเทศ

- องค์ประกอบของความปลอดภัยระบบสารสนเทศที่มีการยอมรับกันว่าการได้มาซึ่งความปลอดภัยของระบบสารสนเทศจะต้องมีองค์ประกอบ 3 สิ่งคือ



การได้มาซึ่งความปลอดภัยระบบสารสนเทศ

- องค์ประกอบของความปลอดภัยระบบสารสนเทศ (security components) - CIA
  - C: Confidentiality
  - I: Integrity
  - A: Availability

การได้มาซึ่งความปลอดภัยระบบสารสนเทศ

- องค์ประกอบของความปลอดภัยระบบสารสนเทศ (security components) - CIA
  - C: Confidentiality - การรักษาความลับ หมายถึงการรักษาหรือสงวนสิทธิในการเข้าถึงระบบสารสนเทศหรือระบบคอมพิวเตอร์หรือข้อมูล ของบุคคลซึ่งได้รับอนุญาตเท่านั้น

การได้มาซึ่งความปลอดภัยระบบสารสนเทศ

- องค์ประกอบของความปลอดภัยระบบสารสนเทศ (security components) - CIA
  - I: Integrity - การรักษาความครบถ้วนสมบูรณ์ หมายถึงการรักษาข้อมูลคอมพิวเตอร์ หรือ ข้อมูลอิเล็กทรอนิกส์ไว้ในสภาพสมบูรณ์ ขณะที่มีการใช้งาน การประมวลผล การโอน หรือการเก็บรักษา มิให้มีการแก้ไข เปลี่ยนแปลง หรือทำลายสารสนเทศ โดยไม่ได้รับอนุญาตหรือโดยไม่ชอบ

การได้มาซึ่งความปลอดภัยระบบสารสนเทศ

- องค์ประกอบของความปลอดภัยระบบสารสนเทศ (security components) - CIA
  - A: Availability - การรักษาความพร้อมใช้ หมายความว่า การจัดทำให้ระบบสารสนเทศหรือระบบคอมพิวเตอร์นั้น สามารถทำงาน ใช้งาน หรือเข้าถึงได้ในเวลาที่ต้องการ

การได้มาซึ่งความปลอดภัยระบบสารสนเทศ

- ตัวอย่างการรักษาความปลอดภัยระบบสารสนเทศ ศปก.ทร.
  - Confidentiality - ข้อมูลในระบบสารสนเทศของ ศปก.ทร. (C3I) เป็นข้อมูลที่มีชั้นความลับ และจะต้องเก็บรักษาให้เป็นความลับ
  - Integrity - ข้อมูลในระบบสารสนเทศของ ศปก.ทร. (C3I) จะต้องมีความถูกต้องและไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต
  - Availability - ระบบสารสนเทศของ ศปก.ทร. (C3I) จะต้องมีความพร้อมใช้ตลอดเวลา

การวิเคราะห์ความเสี่ยงด้านความปลอดภัย

การวิเคราะห์ความเสี่ยงด้านความปลอดภัย

- ภัยต่อระบบสารสนเทศ มีหลายประเภท
  - ภัยต่อ hardware
  - ภัยต่อ data/information/software
  - ภัยต่อการทำงานของระบบ

การวิเคราะห์ความเสี่ยงด้านความปลอดภัย

- ภัยต่อ hardware
  - ภัยธรรมชาติ
  - ไฟไหม้
  - ไฟดับ ไฟตก
  - อุปกรณ์ถูกทำลาย
  - อุปกรณ์ถูกจารกรรม

การวิเคราะห์ความเสี่ยงด้านความปลอดภัย

- ภัยต่อ data/information/software
  - การจารกรรมข้อมูล
  - การหลอกลวง (social engineering)
  - การลักลอบเปลี่ยนแปลงข้อมูล
  - การทำลายข้อมูล
  - virus/ worm/ malware
  - ข้อผิดพลาดในซอฟท์แวร์ (bug)

การวิเคราะห์ความเสี่ยงด้านความปลอดภัย

- ภัยต่อการทำงานของระบบ
  - ยิงให้ล่ม (Denial-of-Service: DoS)
    - ใช้จุดอ่อนที่ซอฟท์แวร์มี bug ทำให้ระบบล่ม
    - ใช้เครื่องหลายๆเครื่องเรียกใช้บริการพร้อมกัน
    - เดา password จนระบบ lock

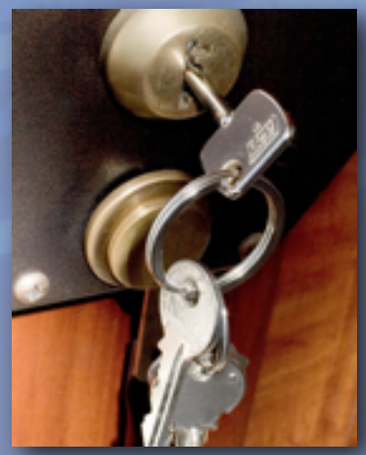
จัดเรียงลำดับความเสี่ยง/หาวิธีแก้ไขปัญหา

การดำเนินการเกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศของกองทัพเรือ

การดำเนินการของ ทร. (โดย สสท.ทร.)

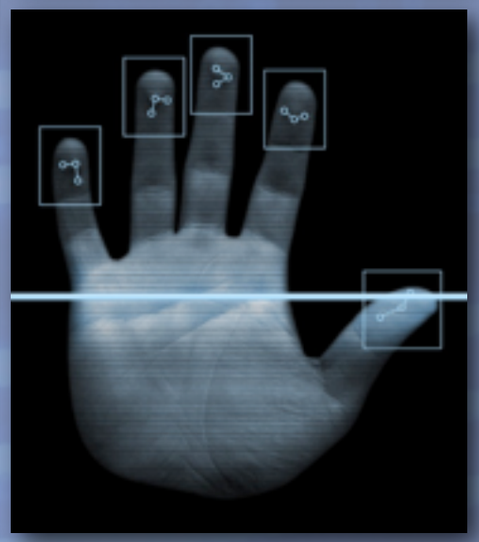
- ภัยธรรมชาติ
  - การสำรองข้อมูล

- ปัญหาเรื่องไฟฟ้า (ไฟดับ ไฟตก)
  - ติดตั้งอุปกรณ์สำรองไฟ (UPS)



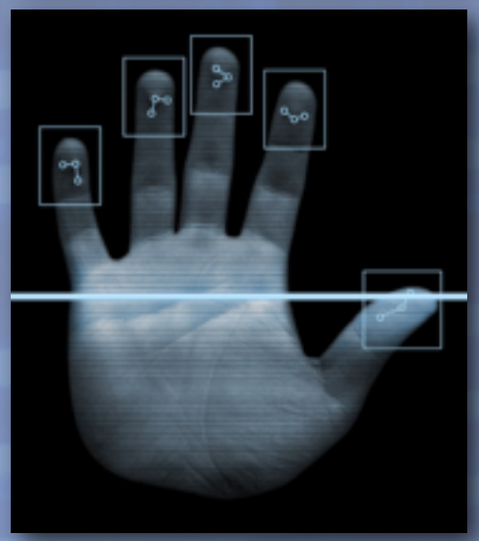
- การทำลายอุปกรณ์/ การจารกรรมอุปกรณ์
  - การรักษาความปลอดภัยทางกายภาพ - ล็อคห้อง จัดเวรยาม

การดำเนินการของ ทร. (โดย สสท.ทร.)



- การจารกรรมข้อมูล
- มาตรการควบคุมการเข้าถึง - พิสูจน์สิทธิ เพื่อยืนยันว่าบุคคลดังกล่าวมีสิทธิในการเข้าถึงระบบหรือข้อมูล
  - username and password
  - biometric, smart card or key card
  - multi-factor authentication

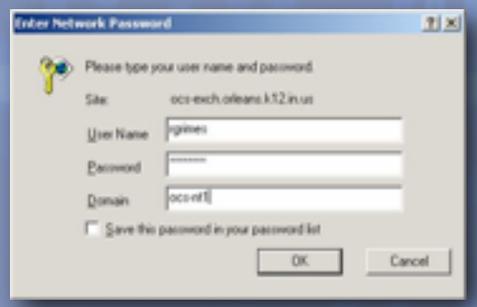
การดำเนินการของ ทร. (โดย สสท.ทร.)



- การจารกรรมข้อมูล
  - การเข้ารหัสข้อมูล (Cryptography) - ทำให้ข้อมูลอยู่ในรูปแบบที่ไม่สามารถใช้ประโยชน์ได้หากไม่รู้วิธี (Encryption) และหากรู้วิธีสามารถทำให้กลับมาอยู่ในรูปแบบที่ใช้ประโยชน์ได้ (Decryption)

การดำเนินการของ ทร. (โดย สสท.ทร.)

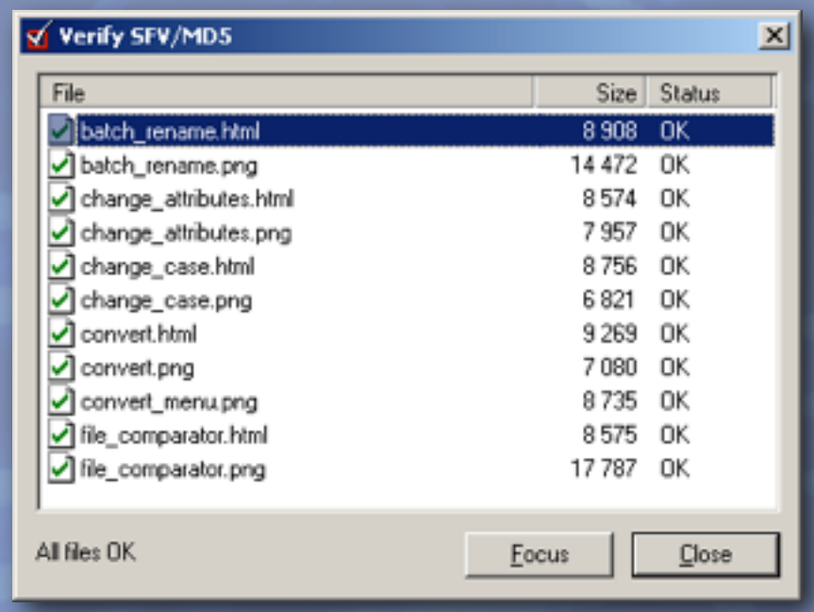
- การลวง (Social Engineering)

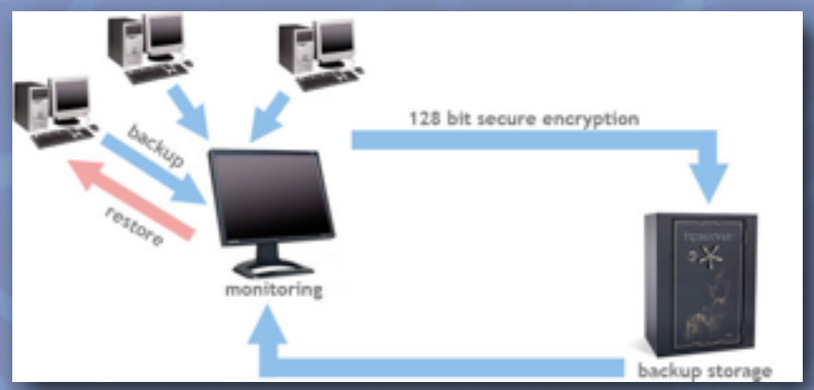


- การพิสูจน์ตัวตน และพิสูจน์สิทธิ - เพื่อยืนยันว่าบุคคลดังกล่าวเป็นบุคคลที่มีสิทธิเข้าถึงจริง

- username and password
- biometric, smart card or key card
- multi-factor authentication

การดำเนินการของ ทร. (โดย สสท.ทร.)





- การลักลอบแก้ไขเปลี่ยนแปลงข้อมูล (data alteration) การทำลายข้อมูล (data destruction)
- checksum - ลายมือของข้อมูล (data fingerprint) ถ้าข้อมูลเปลี่ยน fingerprint ก็จะเปลี่ยน
- advance checksum - ลายมือชื่ออิเล็กทรอนิกส์ (digital signature)
- Backup - on-site, off-site

การดำเนินการของ ทร. (โดย สสท.ทร.)

- ดูแลความปลอดภัยทั้งหมดในศูนย์ข้อมูลสารสนเทศกองทัพเรือ (data center)
- ดูแลและให้คำแนะนำเกี่ยวกับความปลอดภัยระบบสารสนเทศของหน่วยใน ทร.
- ดูแลความปลอดภัยช่องทางเชื่อมต่อเครือข่ายสารสนเทศ ทร.

การดำเนินการของ ทร. (โดย สสท.ทร.)

- กำหนดนโยบายการดำเนินการด้านการรักษาความปลอดภัยระบบสารสนเทศ
- ร่างระเบียบการรักษาความปลอดภัยระบบสารสนเทศ
- กำหนดแนวทางการใช้งานระบบสารสนเทศและมาตรการต่างๆ เพิ่มเติม
- ตรวจสอบการปฏิบัติของหน่วย

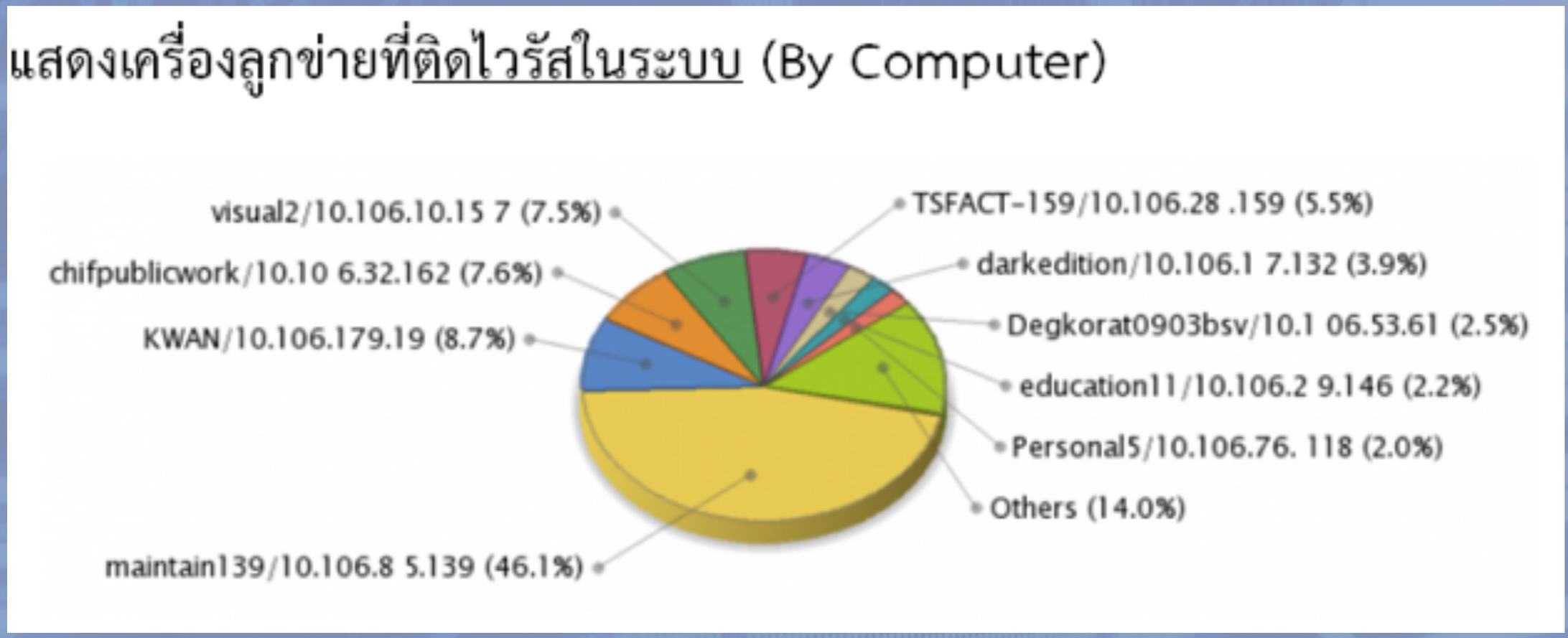
การดำเนินการของ ทร. (โดย สสท.ทร.)

- จัดหาอุปกรณ์หรือซอฟท์แวร์ที่เกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศอย่างเหมาะสม
- ฝึกอบรมเจ้าหน้าที่/ สร้างความตระหนักรู้ให้กับข้าราชการ ทร. ที่ต้องใช้งานระบบสารสนเทศ
- ตรวจสอบ/เฝ้าระวัง การใช้งานที่อาจเป็นภัยต่อระบบ

การดำเนินการของ ทร. (โดย สสท.ทร.)

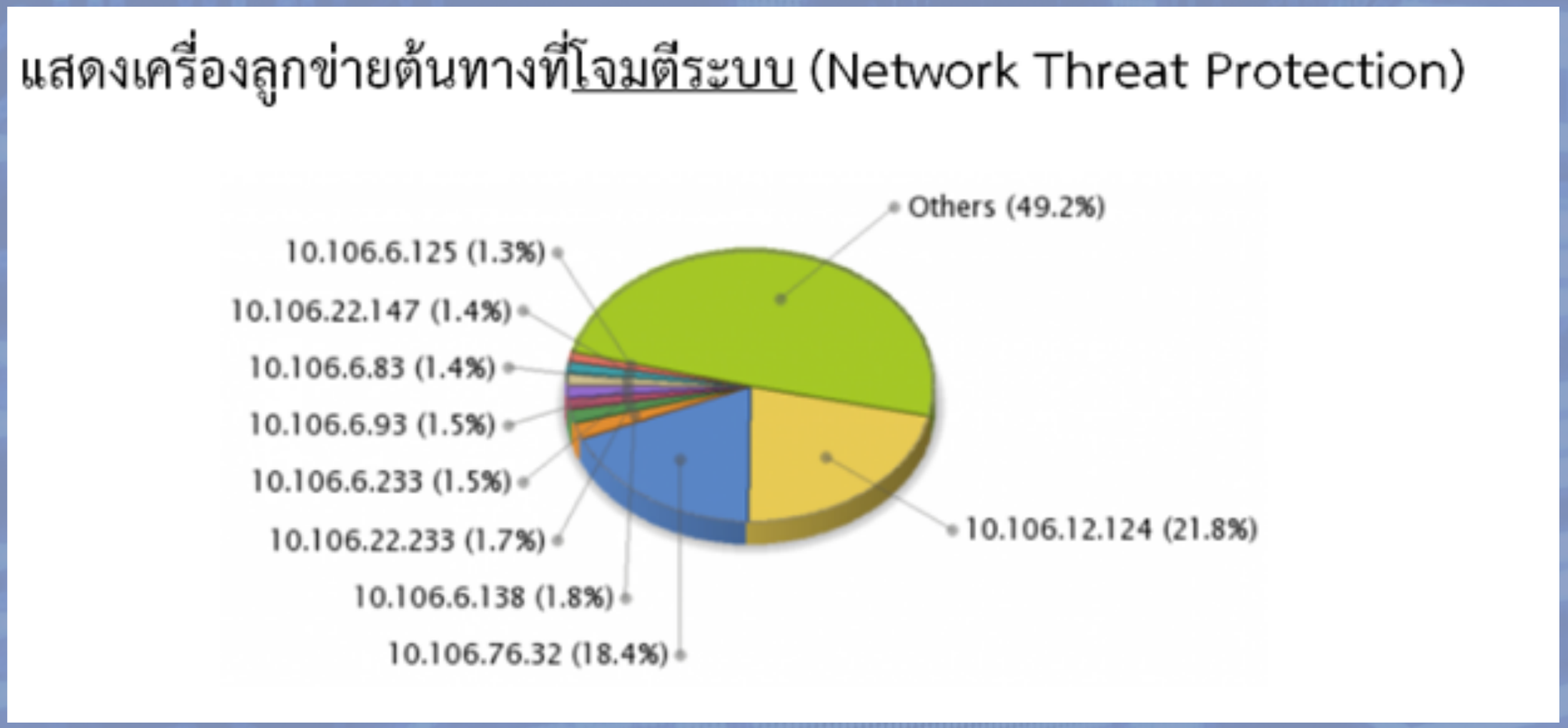
- จัดทำแนวทาง/คู่มือการติดตั้ง การใช้งานอุปกรณ์/ซอฟท์แวร์ที่เกี่ยวข้องกับการ รปภ.สารสนเทศ
- Gateway/Firewall hardening
- File Sharing
- Antivirus
- Software update

การดำเนินการของ ทร. (โดย สสท.ทร.)



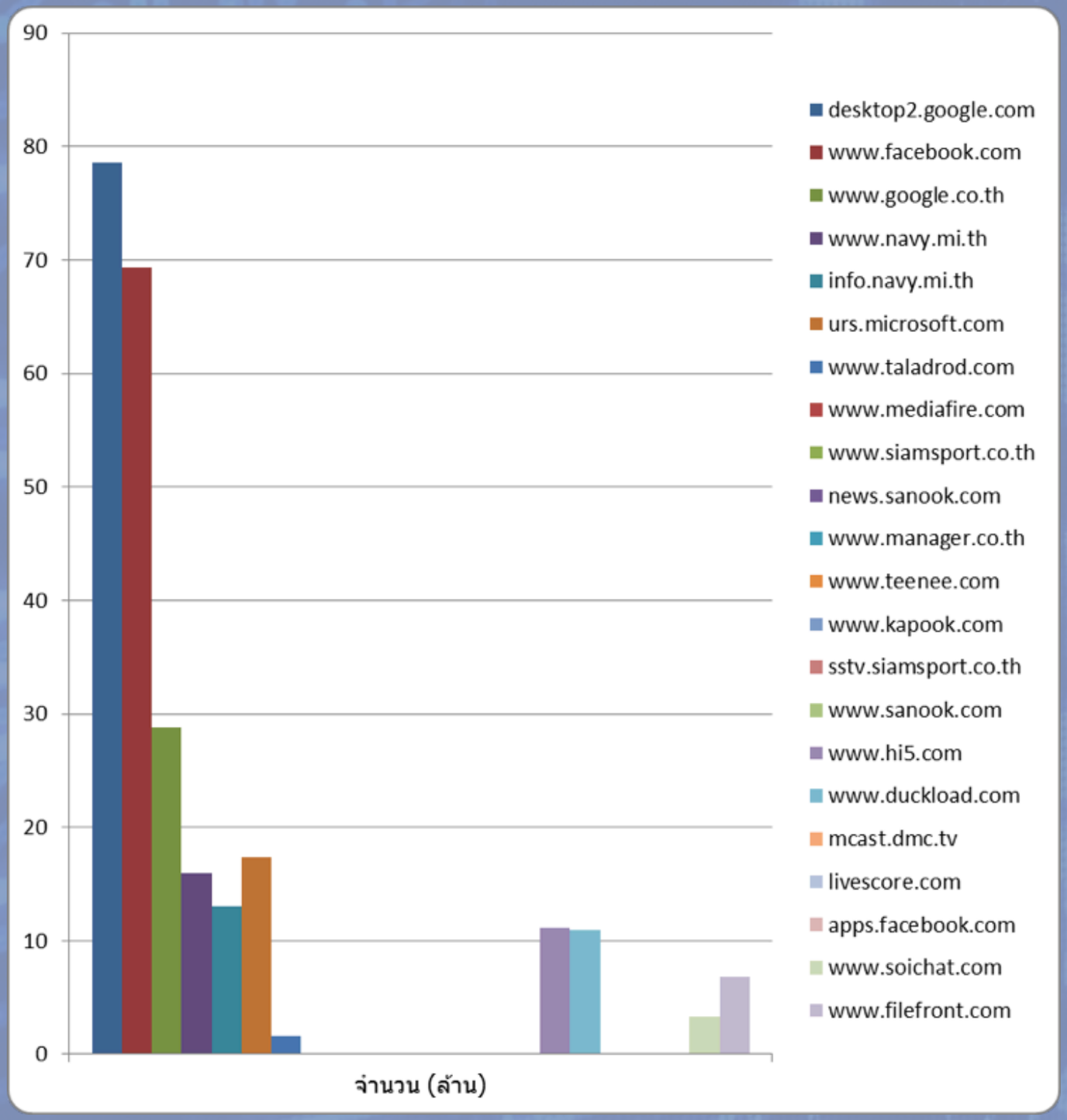
แสดง 10 อันดับเครื่องที่ติดมัลแวร์สูงสุดในเครือข่าย ทร.

การดำเนินการของ ทร. (โดย สสท.ทร.)



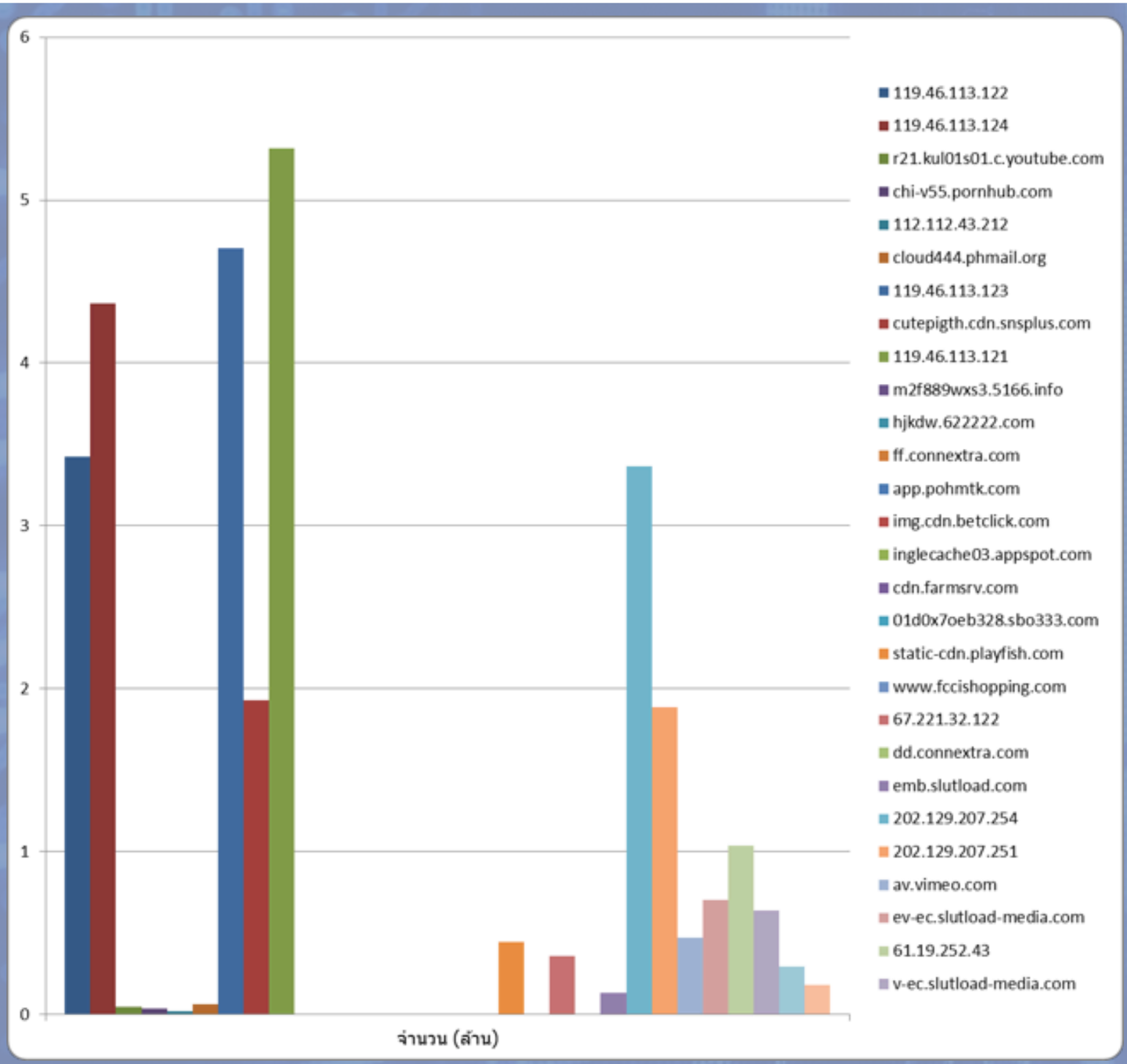
แสดง 10 อันดับเครื่องที่แพร่ระบาดมัลแวร์สูงสุดในเครือข่าย ทร.

การดำเนินการของ ทร. (โดย สสท.ทร.)



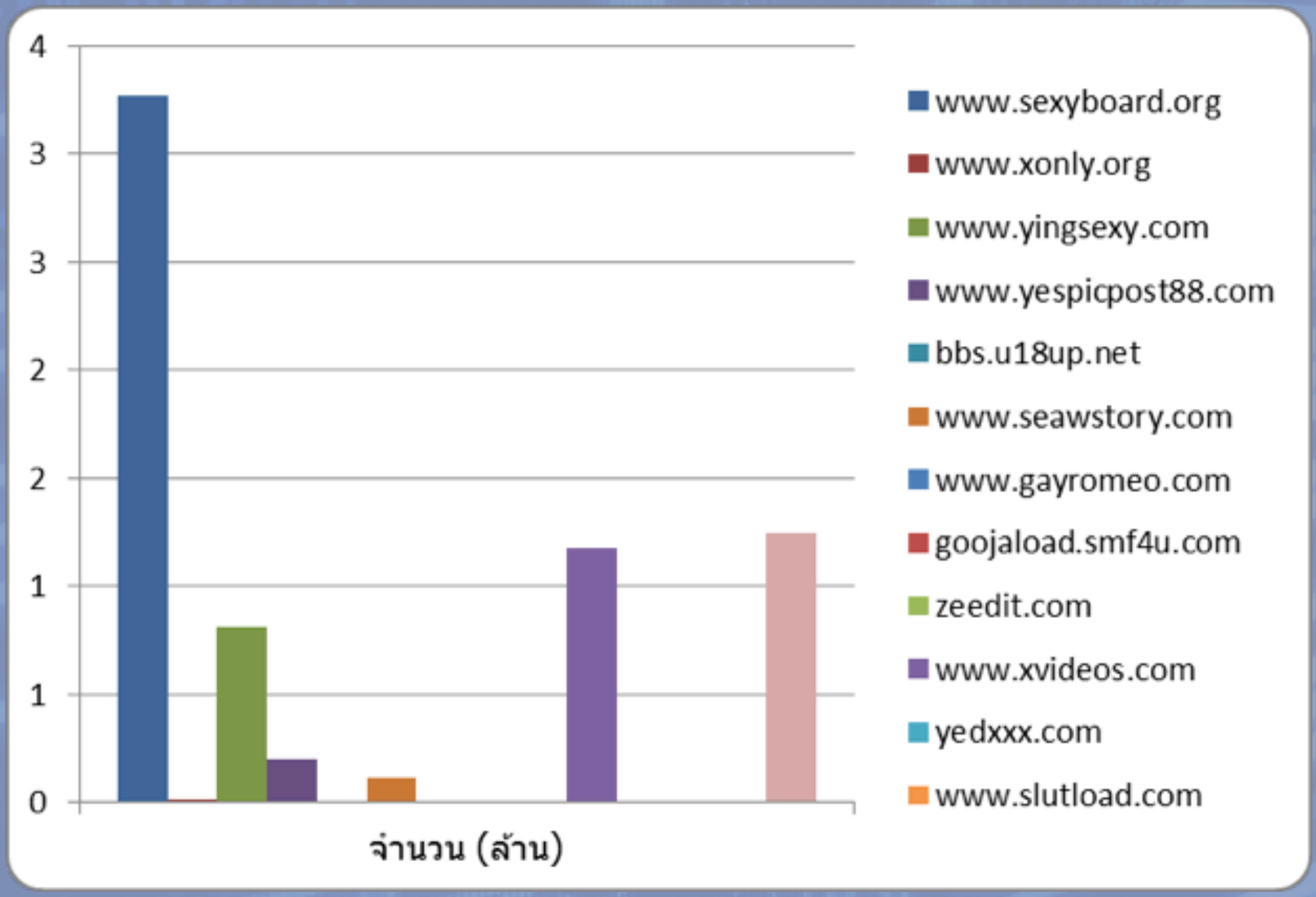
แสดงสถิติเว็บไซต์ที่มีการใช้งานมากที่สุดจากเครือข่าย ทร.

การดำเนินการของ ทร. (โดย สสท.ทร.)



แสดงสถิติเว็บไซต์ที่มีความเสี่ยงด้านความปลอดภัย และถูกเข้าถึงใช้งานมากที่สุดจากเครือข่าย ทร.

การดำเนินการของ ทร. (โดย สสท.ทร.)



การดำเนินการของ ทร. (โดย สสท.ทร.)

Name	IP Address	Operating System	Installed/Not Applic...	Last Status Report
chuksamet2	10.106.84.207	Windows XP Professional	0%	Not yet reported
person2	10.106.84.224	Windows XP Professional	99%	2/10/2010 7:18 AM
oacdc	10.106.84.224	Windows XP Professional	96%	9/29/2009 8:03 AM
onbw1	10.106.84.224	Windows XP Professional	98%	11/26/2009 8:19 AM
illusion-33baa0	10.106.84.224	Windows XP Professional	0%	Not yet reported
illusion-d7092e	10.106.84.224	Windows XP Professional	99%	2/12/2010 7:50 AM
acdcb	10.106.84.224	Windows XP Professional	99%	2/12/2010 8:25 AM
microsof-a8f410	10.106.84.224	Windows XP Professional	98%	12/24/2009 8:03 AM
ส่งกำลัง4กรม	10.106.84.225	Windows XP Professional	100%	2/12/2010 2:29 PM
fasteros-8rjcdu	10.106.84.28	Windows XP Professional	99%	2/12/2010 9:02 AM
illusion-b51a41	10.106.84.28	Windows XP Professional	99%	2/12/2010 9:25 AM
eng01	10.106.84.28	Windows XP Professional	99%	2/12/2010 10:02 AM
microsoft	10.106.84.66	Windows XP Professional	0%	Not yet reported
vijarn	10.106.86.140	Windows XP Professional	99%	2/11/2010 7:31 PM
pjonsek	10.106.91.112	Windows XP Professional	98%	12/4/2009 8:14 AM

chuksamet2

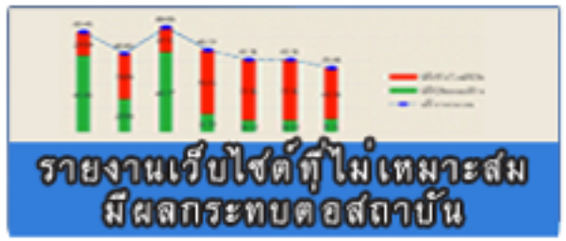
รายละเอียดเพิ่มเติม

http://cybersecurity.navy.mi.th

http://security.navy.mi.th

NAVAL INFORMATION SYSTEMS SECURITY

@หน้าหลัก | @สงครามสารสนเทศ | @สงครามอิเล็กทรอนิกส์ | @การกระทำผิดเกี่ยวกับคอมพิวเตอร์ | @ความรู้ด้านมัลแวร์ | @ความรู้ด้านคอมพิวเตอร์



เอกสาร/ระเบียบ/แบบฟอร์ม

- เอกสารเผยแพร่สำหรับการรักษาความปลอดภัยระบบสารสนเทศในปัจจุบัน โดย กปท.สสท.ทร.

ระเบียบ และแนวทางที่เกี่ยวข้องกับการปฏิบัติการเครือข่ายคอมพิวเตอร์

ระเบียบ ทร. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔

สำเนา

ระเบียบกองทัพเรือ

ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ

พ.ศ.๒๕๕๔

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของกองทัพเรือ เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกองทัพเรือว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

บรรดาระเบียบและคำสั่งอื่นใดของกองทัพเรือในส่วนที่กำหนดไว้แล้วในระเบียบนี้ หรือซึ่งขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๓ การดำเนินการรักษาความปลอดภัยตามระเบียบนี้ ให้ยึดถือและปฏิบัติตามระเบียบ

- ประกอบด้วย ๙ หมวด ดังนี้
  - หมวด ๑ กล่าวถึง จุดมุ่งหมายของระเบียบ หน้าที่ของส่วนราชการ (นขต.ทร. และหน่วยเฉพาะกิจ ทร.) ที่จะต้องมีการดำเนินการกำหนดมาตรการการรักษาความปลอดภัยระบบสารสนเทศของตน และแจ้งให้ สสท.ทร. ทราบ รวมถึงการกำหนดให้ จก.สสท.ทร. ในฐานะผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของ ทร.

ระเบียบ ทร. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔

- ประกอบด้วย ๙ หมวด ดังนี้
  - หมวด ๒ กล่าวถึง แนวทางการรักษาความปลอดภัยเกี่ยวกับบุคคลที่เกี่ยวข้องกับระบบสารสนเทศ การตรวจสอบความไว้วางใจบุคคล การอบรมหรือชี้แจงเรื่องการรักษาความปลอดภัย การมอบหมายหน้าที่เกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศ หน้าที่ของเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของหน่วย

ระเบียบ ทร. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔

- ประกอบด้วย ๙ หมวด ดังนี้
  - หมวด ๓ กล่าวถึง แนวทางการรักษาความปลอดภัยเกี่ยวกับอาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ การกำหนดพื้นที่ตั้งระบบสารสนเทศเป็นพื้นที่หวงห้าม การปฏิบัติในเวลาฉุกเฉิน การจัดทำแผนรับสถานการณ์ฉุกเฉิน

ระเบียบ ทร. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔

- ประกอบด้วย ๙ หมวด ดังนี้
  - หมวด ๔ กล่าวถึง การจัดการการรักษาความปลอดภัยระบบสารสนเทศ ให้มีระดับสมดุลกับความเสี่ยงของระบบสารสนเทศที่ประเมินได้ อำนาจหน้าที่ของ ผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพเรือ

- ประกอบด้วย ๙ หมวด ดังนี้
  - หมวด ๕ กล่าวถึง **การรักษาความปลอดภัยคอมพิวเตอร์พร้อมโปรแกรม** ที่ใช้งานและเชื่อมต่อกับระบบสารสนเทศ ทร. การกำหนดผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์ การจัดทำทะเบียนผู้ใช้งาน การจัดการชั้นความลับของสิ่งบันทึกข้อมูล การจัดการกับข้อมูลในเครื่องคอมพิวเตอร์หากนำไปซ่อมบำรุงหรือรุจำหน่าย

- ประกอบด้วย ๙ หมวด ดังนี้
  - หมวด ๖ กล่าวถึง **การรักษาความปลอดภัยการพัฒนาโปรแกรม หรือระบบสารสนเทศ ที่หน่วยพัฒนาขึ้น และมีการเชื่อมต่อกับเครือข่ายสารสนเทศ ทร.** ให้เป็นไปตามหลักการพัฒนาอย่างปลอดภัย **และต้องมีการขออนุญาต ผอ.รักษาความปลอดภัยระบบสารสนเทศ ทร. ก่อน**

- ประกอบด้วย ๙ หมวด ดังนี้
  - หมวด ๗ กล่าวถึง **การรักษาความปลอดภัยระบบสารสนเทศ** เพื่อควบคุมการรั่วไหลของความลับ และการป้องกันการทำลายข้อมูลสารสนเทศ **โดยกำหนดมาตรการควบคุมและป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต**

- ประกอบด้วย ๙ หมวด ดังนี้
  - หมวด ๘ กล่าวถึง **การจัดการข้อมูลสารสนเทศที่มีชั้นความลับ** โดยกล่าวถึงการปฏิบัติของผู้ที่มีส่วนเกี่ยวข้องกับการแสดงชั้นความลับของสารสนเทศ การปรับและยกเลิกชั้นความลับของข้อมูล

- ประกอบด้วย ๙ หมวด ดังนี้
  - หมวด ๙ กล่าวถึง **การปฏิบัติเมื่องมีการละเมิดการรักษาความปลอดภัย** โดยกล่าวถึงการดำเนินการของเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของหน่วยในการลดความเสียหายเบื้องต้น การรายงานต่อหัวหน้าหน่วย การสำรวจความเสียหาย และการรายงานสรุปเหตุการณ์ต่อ ผอ.รักษาความปลอดภัยระบบสารสนเทศ ทร. ทราบ รวมถึงการดำเนินการสอบสวน ลงโทษผู้รับผิดชอบและผู้กระทำความผิด และการดำเนินการป้องกัน

แนวทางการใช้งานระบบสารสนเทศของกองทัพเรือ

แนวทางการใช้งานระบบสารสนเทศของกองทัพเรือ

อาศัยอำนาจตามข้อ ๒๓ ของระเบียบกองทัพเรือ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ จึงกำหนดแนวทางการใช้งานระบบสารสนเทศของกองทัพเรือ เพื่อเป็นแนวทางให้ข้าราชการ ทร. ยึดถือปฏิบัติ เพื่อให้การใช้งานระบบสารสนเทศเป็นไปด้วยความเรียบร้อย ปลอดภัย คุ้มค่า และเกิดประโยชน์สูงสุดต่อทางราชการ

ข้อ ๑ ข้อปฏิบัติ

๑.๑ การรักษาความปลอดภัยระบบสารสนเทศ ทร.

๑.๑.๑ ผู้ใช้สามารถดาวน์โหลด ระเบียบ ทร. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔ มาตรการและแนวทางที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศ ได้จากเว็บไซต์ **“ข้อมูลด้านความปลอดภัยระบบสารสนเทศ”** (http://iwoc.ncit.navy.mi.th)

๑.๑.๒ เครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบสารสนเทศ ทร. ต้องติดตั้งซอฟท์แวร์ป้องกันมัลแวร์ (มัลแวร์หมายถึงซอฟท์แวร์ไม่พึงประสงค์ที่เป็นภัยต่อระบบสารสนเทศ เช่น ไวรัสคอมพิวเตอร์ หนอนอินเทอร์เน็ต เป็นต้น) ที่ทาง ทร. จัดหา โดยสามารถขอรับการติดตั้งได้จากผู้ดูแลระบบของหน่วย หรือสามารถ

แนวทางการใช้งานระบบสารสนเทศของกองทัพเรือ

๑.๖ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑.๖.๑ กองทัพเรือส่งเสริมให้ ข้าราชการ และ พนักงานราชการ ของ ทร. ใช้งานระบบเครือข่ายสังคมออนไลน์อย่างมีความรับผิดชอบ เพื่อการประชาสัมพันธ์ภารกิจและกิจกรรมต่างๆ ของกองทัพเรือ

๑.๖.๒ ในการใช้งานระบบเครือข่ายสังคมออนไลน์ ผู้ใช้ ควรตรวจสอบข้อมูลหรือความคิดเห็นว่ามีความถูกต้อง ไม่เปิดเผยข้อมูลที่มีชั้นความลับ และต้องไม่กระทบต่อการดำเนินงานของ ทร. เช่นการเปิดเผยตำแหน่งที่ตั้งทางทหาร เรือ อาวุธยุทโธปกรณ์ รวมถึงแผนการปฏิบัติทางทหาร

๑.๖.๓ ผู้ใช้ ควรตระหนักว่าการเปิดเผยข้อมูลหรือการแสดงความคิดเห็นในระบบเครือข่ายสังคมออนไลน์นั้น ผู้ใช้จะไม่สามารถยกเลิกเปิดเผยข้อมูลดังกล่าวได้ ดังนั้นควรมีความระมัดระวังในการเปิดเผยข้อมูล เนื่องจากอาจจะมีผลกระทบต่อผู้เปิดเผยเอง หน่วยงาน และ ทร. ในภาพรวมได้

๑.๖.๔ การแสดงความคิดเห็นในระบบเครือข่ายสังคมออนไลน์ ผู้ใช้จะต้องแจ้งอย่างชัดเจนว่าความคิดเห็นดังกล่าว เป็นความคิดเห็นส่วนบุคคล ไม่ใช่ความคิดเห็นของ ทร. การแสดงความคิดเห็นอย่างเป็นทางการของ ทร. จะกระทำโดยหน่วยงานที่ได้รับมอบหมายโดย ทร. ให้ทำการประชาสัมพันธ์อย่างเป็นทางการเท่านั้น

๑.๖.๕ ในการใช้งานระบบเครือข่ายสังคมออนไลน์ ผู้ใช้ ควรใช้บัญชีจดหมายอิเล็กทรอนิกส์ส่วนตัวเท่านั้น

๑.๖.๖ ผู้ใช้ควรมีความระมัดระวังในการให้สิทธิ์การเข้าถึงข้อมูลของตนในระบบเครือข่ายสังคมออนไลน์ เช่นการตอบรับการเป็นเพื่อน (Friend) การเป็นผู้ติดตาม (Follower) เนื่องจากผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลส่วนตัวที่อาจส่งผลกระทบให้เกิดความเสี่ยงด้านการรักษาความปลอดภัยได้ นอกจากนี้ยังแนะนำให้ผู้ใช้ทำการตรวจสอบการตั้งค่าความปลอดภัยในการใช้งานระบบเครือข่ายสังคมออนไลน์อย่างสม่ำเสมอ

แนวทางการใช้งานระบบสารสนเทศของกองทัพเรือ

๒.๖ การใช้งานระบบเครือข่ายสังคมออนไลน์ (Social Network) ห้ามทำการเปิดเผยข้อมูลหรือเอกสารที่ ทร. ไม่ได้เปิดเผยต่อสาธารณะ ในที่นี้รวมถึงข้อมูลหรือเอกสารที่มีชั้นความลับ เช่นแผนการปฏิบัติการจัดกำลังพล ข้อมูลเกี่ยวกับเรือ อาวุธยุทโธปกรณ์ รวมถึงข้อมูลการติดต่อเช่น หมายเลขโทรศัพท์ บัญชีจดหมายอิเล็กทรอนิกส์ ที่ไม่ได้รับอนุญาตให้เปิดเผยต่อสาธารณะ และข้อมูลอื่นๆ ที่ไม่ควรเปิดเผย หากมีข้อสงสัยเกี่ยวกับการเปิดเผยข้อมูล ควรติดต่อสอบถามกับนายทหารรักษาความปลอดภัยของหน่วยต้นสังกัด

ระบบบริการอินเทอร์เน็ตผ่านเครือข่ายสารสนเทศ ทร. เป็นของกองทัพเรือ กองทัพเรือจะสงวนสิทธิในการดำเนินการใดๆ ในการบันทึกข้อมูลการใช้งานบริการของผู้ใช้ เพื่อการตรวจสอบความเหมาะสมในการใช้งาน การรักษาความปลอดภัย การปฏิบัติตามกฎหมาย ผู้ที่ไม่ปฏิบัติตามแนวทางการใช้งานนี้ สสท.ทร. จะพิจารณาดำเนินการตามลำดับดังนี้

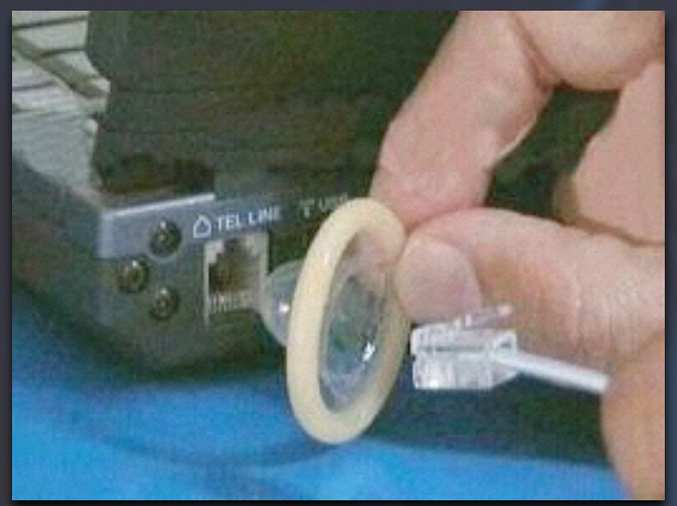
๓.๑ แจ้งเตือนให้รับทราบ

๓.๒ รายงานให้ผู้บังคับบัญชาของผู้ใช้ที่ไม่ปฏิบัติตามทราบ

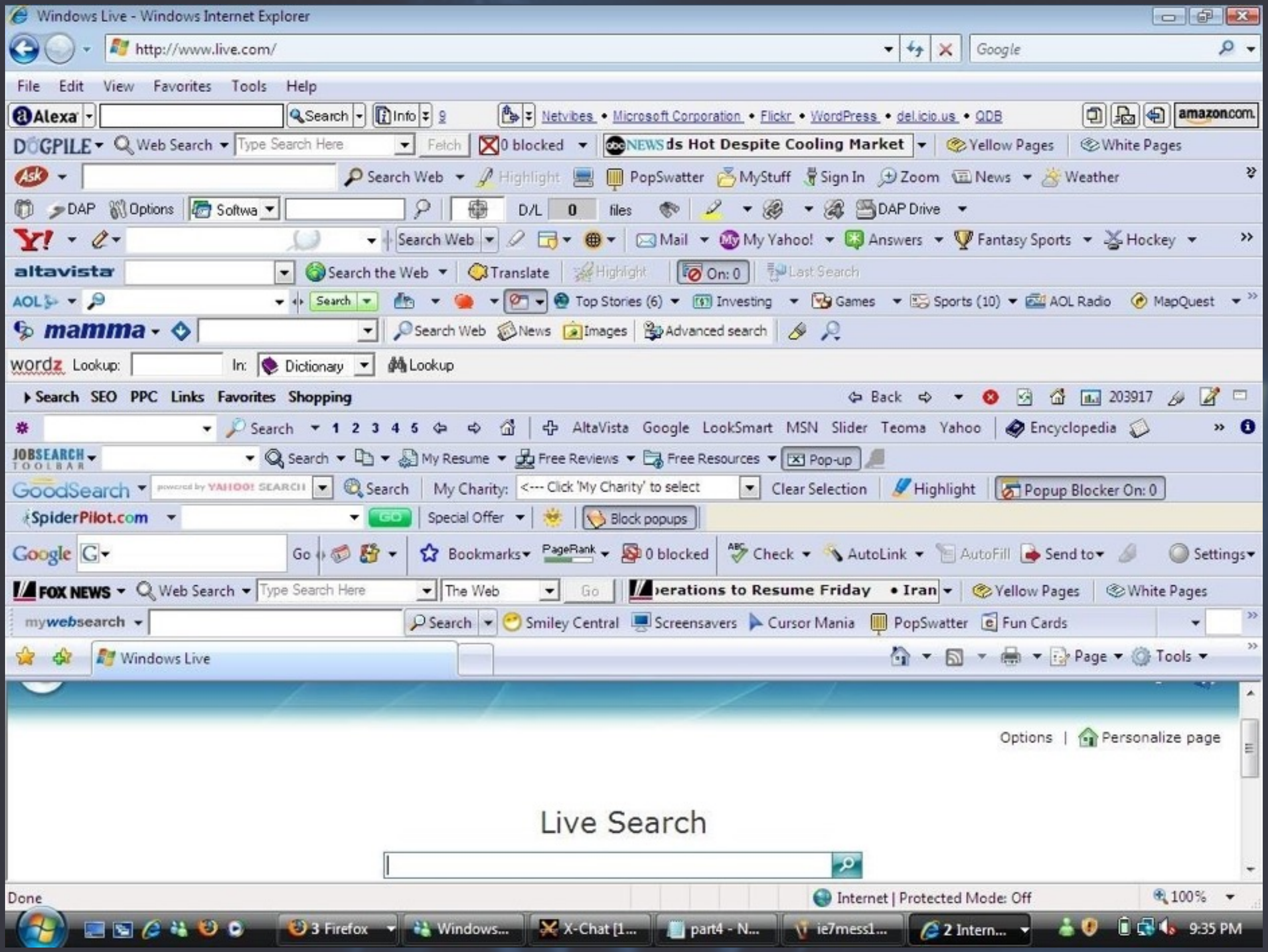
๓.๓ พิจารณาตัดสิทธิ์ การใช้บริการอินเทอร์เน็ต และรายงานเป็นลายลักษณ์อักษร ให้ผู้บังคับบัญชาของผู้ใช้ทราบ

สาธิตการ Hack

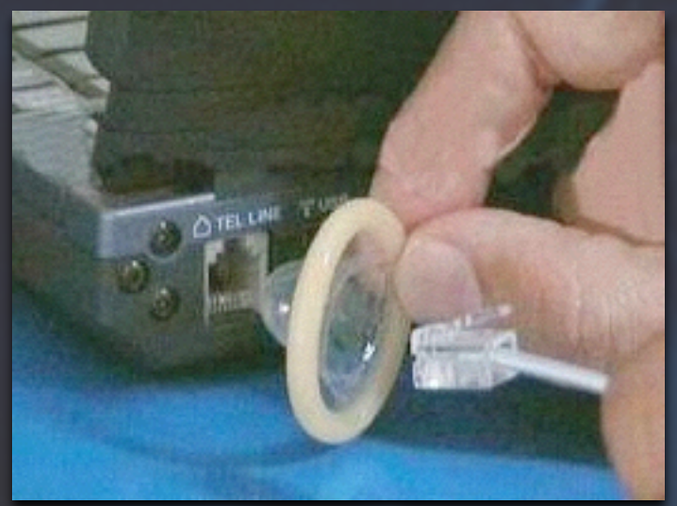
การป้องกันภัยดังกล่าว



- มีความตระหนักรู้เกี่ยวกับเรื่องความปลอดภัยระบบสารสนเทศ (Security Awareness) - No more Mr.Yes man!!

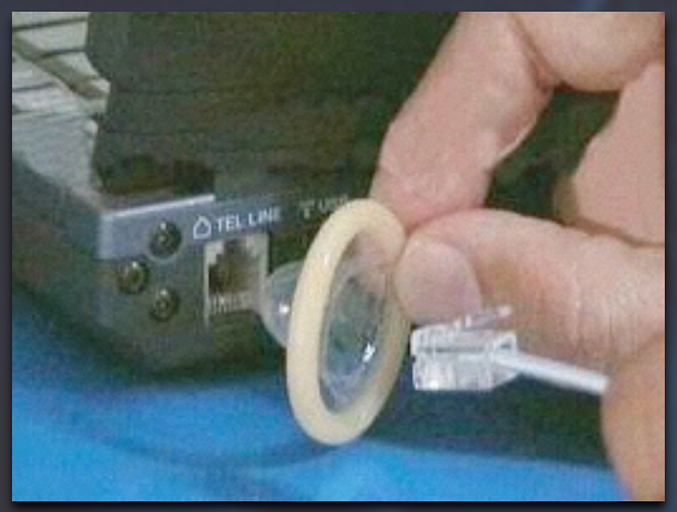

Windows Live - Windows Internet Explorer
http://www.live.com/
Google
File Edit View Favorites Tools Help
Alexa Search Info 9 Netvibes • Microsoft Corporation • Flickr • WordPress • del.icio.us • QDB amazon.com
DOGPILE Web Search Type Search Here Fetch 0 blocked NEWS ds Hot Despite Cooling Market Yellow Pages White Pages
Ask Search Web Highlight PopSwatter MyStuff Sign In Zoom News Weather
DAP Options Softwa D/L 0 files DAP Drive
Y! Search Web Mail My Yahoo! Answers Fantasy Sports Hockey
altavista Search the Web Translate Highlight On: 0 Last Search
AOL Search Top Stories (6) Investing Games Sports (10) AOL Radio MapQuest
mamma Search Web News Images Advanced search
wordz Lookup: In: Dictionary Lookup
Search SEO PPC Links Favorites Shopping Back 203917
Search 1 2 3 4 5 AltaVista Google LookSmart MSN Slider Teoma Yahoo Encyclopedia
JOBSEARCH TOOLBAR Search My Resume Free Reviews Free Resources Pop-up
GoodSearch powered by YAHOO! SEARCH Search My Charity: <--- Click 'My Charity' to select Clear Selection Highlight Popup Blocker On: 0
SpiderPilot.com GO Special Offer Block popups
Google Go Bookmarks PageRank 0 blocked Check AutoLink AutoFill Send to Settings
FOX NEWS Web Search Type Search Here The Web Go erations to Resume Friday • Iran Yellow Pages White Pages
mywebsearch Search Smiley Central Screensavers Cursor Mania PopSwatter Fun Cards
Windows Live
Page Tools
Options | Personalize page
Live Search
Done
Internet | Protected Mode: Off
100%
3 Firefox
Windows...
X-Chat [1...
part4 - N...
ie7mess1...
2 Intern...
9:35 PM

การป้องกันภัยดังกล่าว



- มีความตระหนักรู้เกี่ยวกับเรื่องความปลอดภัยระบบสารสนเทศ (Security Awareness) - No more Mr.Yes man!!
- Security software - firewall, antimalware (malware = malicious software)

การป้องกันภัยดังกล่าว



- Secure App Development - ตรวจสอบข้อมูลใน form ต่างๆ ว่ามีอักขระพิเศษที่ไม่ควรมีหรือไม่
- Software update - OS, applications
- Application Firewall

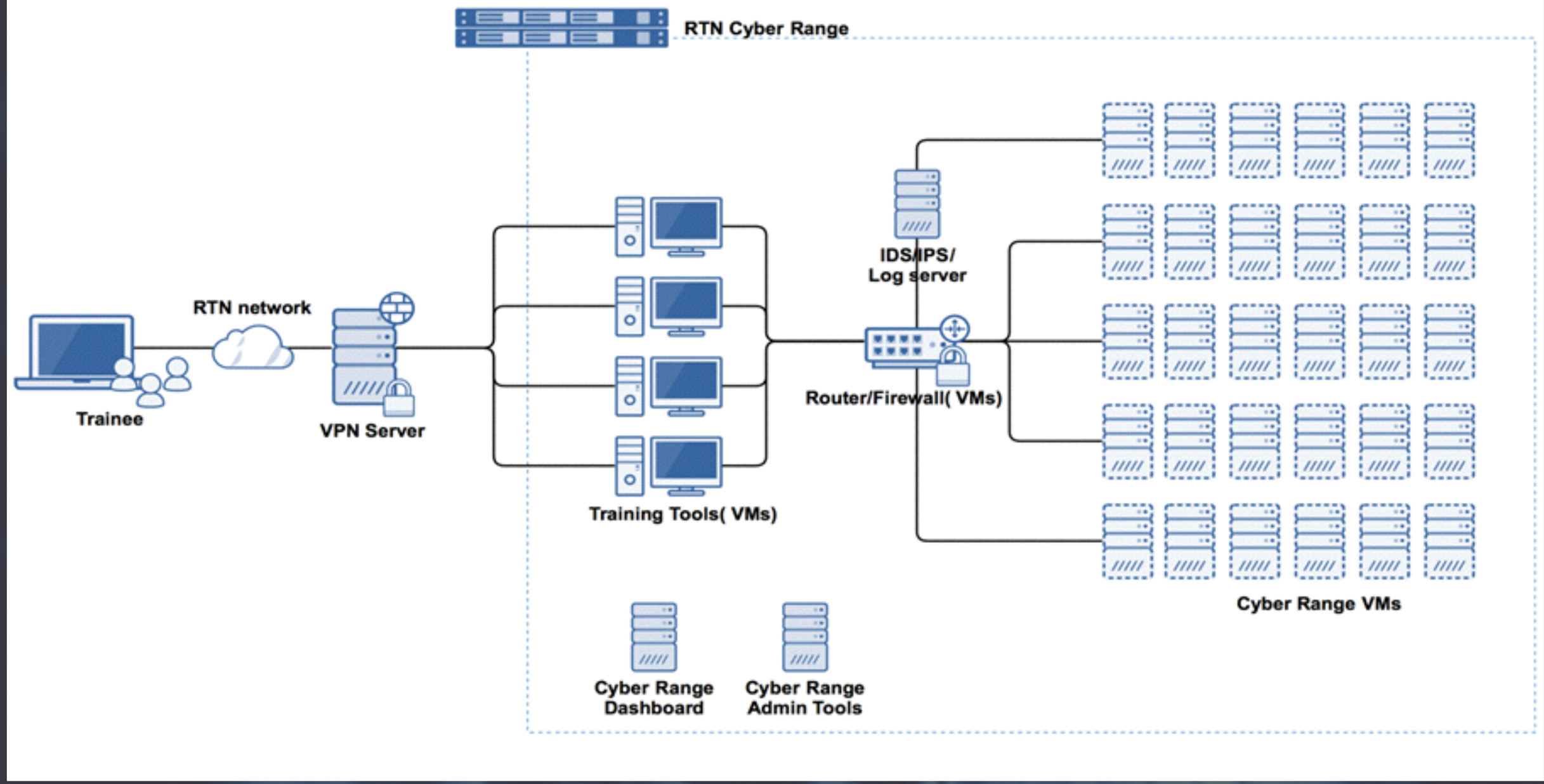
Navy Cyber Contest

ความเป็นมา

- ทร. จัดหาระบบจำลองการฝึกปฏิบัติการเครือข่ายคอมพิวเตอร์ ตั้งแต่ปี งป.๕๗ ปัจจุบันเป็นระยะที่ ๓
- โดยมีวัตถุประสงค์เพื่อ
  - จำลอง Cyber space ที่เหมือนจริง สามารถจำลอง เครื่องคอมพิวเตอร์ ระบบงาน และเครื่องข่าย ทร. จริงได้ เพื่อให้การฝึกสามารถนำไปปรับใช้งานจริงได้ โดยไม่กระทบต่อระบบงานจริง และปรับแต่งสภาพแวดล้อมได้ตามความต้องการ รองรับ การฝึก/อบรม ทางไกล ผ่านเครือข่ายสารสนเทศ ทร.

ความเป็นมา

- โดยมีวัตถุประสงค์เพื่อ (ต่อ)
  - โจทย์ฝึก ครอบคลุมการพัฒนาขีดความสามารถ การป้องกัน (Defense) การโจมตีหาข่าว (Attack and Exploitation) การวิเคราะห์พิสูจน์หลักฐาน (Forensic) กระบวนการบริหารจัดการด้านความปลอดภัย (Cyber Security Operation Center)
  - แนวทางการฝึกและโจทย์ฝึก รองรับการพัฒนาบุคลากร ตามระดับความเชี่ยวชาญ ตั้งแต่ระดับเริ่มต้น ระดับกลาง และระดับสูง ในการฝึกประเภทต่างๆ
  - มีระบบประเมินการฝึก/อบรม ที่เป็นอัตโนมัติ และสามารถเก็บข้อมูลการฝึก สถิติ รายชื่อ ผลการฝึก จัดทำเป็นรายงานการใช้งานระบบฝึกได้ รวมทั้งสามารถออกแบบการฝึก/อบรม สอดคล้องกับแนวทางการฝึก และระดับผู้รับการฝึก/อบรม


RTN Cyber Range
RTN network
Trainee
VPN Server
IDS/IPS/
Log server
Router/Firewall(VMs)
Training Tools(VMs)
Cyber Range VMs
Cyber Range
Dashboard
Cyber Range
Admin Tools

รายละเอียดการจัด

- แข่งขัน ภายใน ทร. (Open)
  - รับสมัคร ระหว่าง ปลายเดือน มิ.ย. - ๑๕ ก.ค.๕๙
  - ทีมละ ๓ นาย
  - ผู้สมัคร เข้ารับการอบรม ระหว่าง ๑ - ๕ ส.ค.๕๙
  - แข่งขันภายใน วันที่ ๕ ส.ค.๕๙

รายละเอียดการจัด

- รอบชิง: จัดวันที่ ๗ ก.ย.๕๙ ณ หอประชุมกองทัพเรือ
- ทีม ๘ ทีมสุดท้ายประกอบด้วย

1. ทีม ทร.
2. ทีม สสท.ทร.
3. ทีม ทบ.
4. ทีม ทอ.
5. ทีม บก.ทท.
6. ทีม กห.
7. ทีมภายนอก
8. ทีมภายนอก