รายงานสถานการณ์แพร่กระจายไวรัส ภายใน มศว

สำหรับ หน่วยงาน

ระหว่างวันที่ 29 กรกฎาคม 2548 ถึง 10 สิงหาคม 2548

รายงานผลการดำเนินการ

ฝ่ายปฏิบัติการและบริการ และฝ่ายระบบคอมพิวเตอร์และเครือข่าย

สิงหาคม 2548

สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ
Computer Center, Srinakharinwirot University

สารบัญ **หน้า**

รายงานสถานการณ์แพร่กระจายไวรัส ภายใน มศว

ความเป็นมาและสาเหตุ

จากการได้รับแจ้งจากคณะวิทยาศาสตร์ และคณะวิศวกรรมศาสตร์ ว่าเครือข่ายภายในอาคาร 19, อาคารคณะวิศวกรรมศาสตร์ และอาคารภาควิชาวิศวกรรมศาสตร์โยธา ไม่สามารถใช้งานบริการผ่านเครือข่ายได้ นับตั้งแต่วันที่ 30 กรกฎาคม 2548 และ 4 สิงหาคม 2548 ตามลำดับ โดยสำนักคอมพิวเตอร์ได้ส่งเจ้าหน้าที่เข้าไปตรวจสอบอุปกรณ์หลักภายในอาคาร พบว่าเครือข่ายภายในอาคาร มีการส่งข้อมูล(package) จำนวนมากมายังอุปกรณ์หลักประจำอาคารจนไม่สามารถรองรับการทำงานได้ ทำให้อุปกรณ์หลักประจำอาคารหยุดการทำงาน และได้ตรวจสอบเครื่องคอมพิวเตอร์พบว่ามีการติดไวรัส

ผลกระทบต่อการใช้งานบนเครือข่ายบัวศรี

- เครือข่ายภายในอาคาร 19 คณะวิทยาศาสตร์ ใช้งานบริการเครือข่ายไม่ได้
- เครือข่ายภายในอาคารคณะวิศวกรรมศาสตร์ และอาคารภาควิชาวิศวกรรมศาสตร์โยธา ใช้งานบริการเครือข่ายไม่ได้
- เครือข่ายอาคารสมเด็จพระเทพฯ ใช้งานเครือข่ายได้ แต่การใช้งานระบบห้องสมุด ได้เป็นบางครั้งบางคราว จะต้องทำการเปิดเครื่องคอมพิวเตอร์ใหม่ทุกครั้ง ที่ใช้งานไม่ได้

วันที่ได้รับแจ้งปัญหา

- คณะวิทยาศาสตร์ ได้รับแจ้ง วันเสาร์ที่ 30 เดือนกรกฎาคม พ.ศ. 2548
- คณะวิศวกรรมศาสตร์ ได้รับแจ้ง วันพฤหัสบดีที่ 4 เดือนสิงหาคม พ.ศ. 2548
- สำนักหอสมุดกลาง ได้รับแจ้ง วันพฤหัสบดีที่ 4 เดือนสิงหาคม พ.ศ. 2548

หน่วยงานที่ได้รับผลกระทบ

ลำดับ	คณะ	อาคาร	อาการ	วันที่ได้รับแจ้ง	วันที่เข้าดำเนินการ	วันที่เริ่มใช้งานได้	สถานภาพ
1.	คณะวิทยาสาสตร์	อาคาร 19	ผู้ใช้งานคอมพิวเตอร์ไม่สามารถใช้งานบนเครือข่ายและอินเทอร์เน็ตภายในอาคาร 19 ได้	30 ก.ค.48	1 ส.ค.48	2 ส.ค.48 (เริ่มใช้งานได้ในบริเวณชั้นที่มีการตรวจสอบแล้ว)	ใช้งานได้ตามปกติ แต่ยังมีเครื่องคอมพิวเตอร์ บางส่วนที่ยังไม่ได้ตรวจสอบ เนื่องจากไม่สามารถเข้าห้องพักได้
2.	คณะวิศวกรรมศาสตร์	อาคารคณะวิศวะ และอาคารภาควิชาวิศวกรรมโยธา	ผู้ใช้งานคอมพิวเตอร์ไม่สามารถใช้งานบนเครือข่ายและอินเทอร์เน็ตภายในอาคารอาคารคณะวิศวะ และอาคารภาควิชาวิศวกรรมโยธา ได้	4 ส.ค.48	4 ส.ค.48	4 ส.ค.48 (เฉพาะอาคารคณะวิศวฯ)	อาคารคณะวิศวฯ ใช้งานได้แล้ว (และอาคารวิศวฯโยธา ใช้งานได้ เกิดจากสายสัญญาณ UTP ชำรุด)
3.	สำนักหอสมุดกลาง	อาคารสมเด็จพระเทพฯ	ปัญหาการใช้งานระบบห้องสมุดได้บ้างไม่ได้บ้าง เป็นระยะๆ	4 ส.ค. 48	5 ส.ค. 48	8 ส.ค. 48	ระบบห้องสมุดใช้งานได้ตามปกติ

การดำเนินการ

- สำนักคอมพิวเตอร์ตรวจสอบอุปกรณ์ และดำเนินการแก้ไข
- สำนักคอมพิวเตอร์ทำหนังสือแจ้งหน่วยงานที่มีปัญหาทราบและขอความร่วมมือให้ความสำคัญในการติดตั้งระบบป้องกันไวรัสบนเครื่องไมโครคอมพิวเตอร์ทุกเครื่อง โดยเฉพาะเครื่องไมโครคอมพิวเตอร์ที่มีการจัดหามาใหม่ และสำนักคอมพิวเตอร์ยินดีให้คำแนะนำในการติดตั้งระบบป้องกันไวรัส พร้อมทั้งส่งคู่มือการดูแลรักษาความปลอดภัยเครื่องคอมพิวเตอร์
- สำนักคอมพิวเตอร์ส่งเจ้าหน้าที่เข้าไปดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่อง หากพบเครื่องคอมพิวเตอร์ติดไวรัส เจ้าหน้าที่จะดำเนินการติดตั้งระบบป้องกันไวรัส ชื่อ OfficeScan และติดตั้ง Windows/Software Update Service (SUS) ซึ่งเป็นระบบที่สำนักคอมพิวเตอร์ให้บริการแก่บุคลากรและหน่วยงาน สำหรับการติดตั้งระบบป้องกันไวรัส และเพื่อปรับปรุงช่องโหว่ของโปรแกรมระบบปฏิบัติการวินโดว์ที่ใช้งานแบบอัตโนมัติ บนเครื่องไมโครคอมพิวเตอร์ ผ่านเครือข่ายบัวศรี

เจ้าหน้าที่ดำเนินการ

เจ้าหน้าที่ดำเนินการแก้ปัญหา จำนวน 10 คน โดยแบ่งทีมดำเนินการแก้ปัญหา จำนวน 9 คน และเจ้าหน้าที่ประสานงานรับเรื่องปัญหา จำนวน 1 คน

อาคาร	คณะ	รายชื่อเจ้าหน้าที่ดำเนินการ
อาคาร 19	คณะวิทยาศาสตร์	• นายวิโรจน์ เตี๋ยอนุกูล • นายถาวร หงษ์ทอง • นายสุนทร แจ่มเมือง • นายสันติ สุขยานันท์ • นายชัยวัฒน์ ช่างกลึง • นายประกิจ ลีลาเชี่ยวชาญกุล • นายไพโรจน์ ผาสุวรรณ์ (ประสานงานรับเรื่องปัญหา)
อาคารคณะวิศวฯ และอาคารภาควิชาวิศวฯ โยธา	คณะวิศวกรรมศาสตร์	• นายสมเกียรติ อินตาสาย
อาคารสมเด็จพระเทพฯ	สำนักหอสมุดกลาง	• นายมหัทธวัฒน์ รักษาเกียรติศักดิ์ • นายนคร บริพนธ์มงคล • นายประกิจ ลีลาเชี่ยวชาญกุล

ผลการดำเนินการ

จากการตรวจสอบพบว่าสาเหตุมาจากเครื่องคอมพิวเตอร์ไม่ได้ติดตั้งระบบป้องกันไวรัส หรือติดตั้งระบบป้องกันไวรัสอื่นๆ แต่ไม่ได้ Update ข้อมูลไวรัสล่าสุด หรือ ไม่ได้ติดตั้งระบบ Windows/Software Update Service (SUS) และขอสรุปผลการดำเนินการแก้ปัญหา **ณ วันที่ 10 สิงหาคม 2548**

คณะ	อาคาร	จำนวนเครื่องคอมพิวเตอร์ตรวจสอบ		จำนวนเจ้าหน้าที่ดำเนินการ	ผลการดำเนินการ
		ทั้งหมด	ติดไวรัส		
คณะวิทยาศาสตร์	อาคาร 19	130	66	5	ใช้งานได้ตามปกติ แต่ยังมีเครื่องคอมพิวเตอร์บางส่วนที่ยังไม่ได้ตรวจสอบ เนื่องจากไม่สามารถเข้าห้องพักได้
คณะวิศวกรรมศาสตร์	อาคารคณะวิศวฯ	44	36	1	อาคารคณะวิศวฯ ใช้งานได้แล้ว (และอาคารวิศวฯ โยธา ใช้งานได้ เกิดจากสายสัญญาณ UTP ชำรุด)
	รวม	174	102		

<u>ข้อเสนอแนะ</u> : กรณีที่หน่วยงานใช้โปรแกรม GoBack เป็นโปรแกรมที่ทำหน้าที่เหมือนกับ Undo Card หรือใช้ Undo Card เมื่อติดตั้งโปรแกรมใดๆ ไปแล้ว เมื่อทำการ Restart เครื่อง แล้ว Window จะกลับมาเหมือนเดิม คือเหมือนไม่ได้ติดตั้งอะไรเลย ดังนั้นจึงไม่แนะนำให้ใช้ โปรแกรมนี้กับเครื่องที่มีการเชื่อมต่อกับระบบเครือข่ายมหาวิทยาลัย เช่น ห้องปฏิบัติการคอมพิวเตอร์ ชั้น 15 อาคาร 19 คณะวิทยาศาสตร์ และห้องปฏิบัติคอมพิวเตอร์ SALI Center สำนักหอสมุดกลาง ประสานมิตร

สำหรับปัญหาการใช้งานระบบห้องสมุด ไม่ได้เป็นระยะๆ นั้น สำนักคอมพิวเตอร์ ได้ส่งเจ้าหน้าที่เข้าไปดำเนินการตรวจสอบและประสานงานกับสำนักหอสมุดกลาง จำนวน 3 คน และขณะนี้ระบบห้องสมุดใช้งานได้ตามปกติแล้ว แต่ยังไม่สามารถสรุปสาเหตุได้ว่าเกิดจากปัญหาการแพร่กระจายไวรัส หรือสาเหตุอื่น <u>จึงเห็นควรให้สำนักหอสมุดกลางนัดผู้เกี่ยวข้อง (เจ้าหน้าที่สำนักหอสมุดกลาง เจ้าหน้าที่สำนักคอมพิวเตอร์ และบริษัทดูแลระบบห้องสมุด) ร่วมกันสรุปประเด็นและสาเหตุที่เกิดขึ้นต่อไป</u>

ปัญหา อุปสรรค และข้อเสนอแนะ

ลำดับ	ปัญหา และอุปสรรค	ข้อเสนอแนะ
1.	บางห้องไม่สามารถเข้าดำเนินการตรวจสอบได้ เนื่องจากห้องพักปิด	หน่วยงานควรมีการประสานงานภายในหน่วยงานเพื่ออำนวยความสะดวกให้กับเจ้าหน้าที่สำนักคอมพิวเตอร์ เข้าไปดำเนินการ
2.	เครื่องคอมพิวเตอร์บางเครื่องไม่มีการติดตั้งระบบป้องกันไวรัส หรือ หรือติดตั้งระบบป้องกันไวรัสอื่นๆ แต่ไม่ได้ Update ข้อมูลไวรัสล่าสุด หรือ ไม่ได้ติดตั้งระบบ Windows/Software Update Service (SUS	• ควรให้หน่วยงานตระหนักความสำคัญในการติดตั้งระบบป้องกันไวรัส และปรับปรุงช่องโหว่ของโปรแกรมระบบปฏิบัติการวินโดว์ที่ใช้งานแบบอัตโนมัติ โดยติดตั้งระบบดังกล่าวที่สำนักคอมพิวเตอร์ให้บริการอยู่ • ควรมีมาตรการและนโยบายในภาพรวมการให้บริการเครื่องคอมพิวเตอร์ภายในมหาวิทยาลัย
3.	กรณีที่หน่วยงานใช้โปรแกรม GoBack เป็นโปรแกรมที่ทำหน้าที่เหมือนกับ Undo Card หรือใช้ Undo Card เมื่อติดตั้งโปรแกรมใดๆ ไปแล้ว เมื่อทำการ Restart เครื่อง แล้ว Window จะกลับมาเหมือนเดิม คือเหมือนไม่ได้ติดตั้งอะไรเลย ดังนั้นจึงไม่แนะนำให้ใช้ โปรแกรมนี้กับเครื่องที่มีการเชื่อมต่อกับระบบเครือข่ายมหาวิทยาลัย เช่น ห้องปฏิบัติการคอมพิวเตอร์ ชั้น 15 อาคาร 19 คณะวิทยาศาสตร์ และห้องปฏิบัติคอมพิวเตอร์ SALI Center สำนักหอสมุดกลาง ประสานมิตร	ไม่แนะนำให้ใช้ โปรแกรมนี้กับเครื่องที่มีการเชื่อมต่อกับระบบเครือข่ายมหาวิทยาลัย เช่น ห้องปฏิบัติการคอมพิวเตอร์ ชั้น 15 อาคาร 19 คณะวิทยาศาสตร์ และห้องปฏิบัติคอมพิวเตอร์ SALI Center สำนักหอสมุดกลาง ประสานมิตร
4.	ขาดกำลังคนในการเข้าดำเนินการตรวจสอบและติดตั้งระบบป้องกันไวรัส เนื่องจากเจ้าหน้าที่สำนักคอมพิวเตอร์ จำนวนหนึ่งได้ลาออกไป	สร้างแรงจูงใจในเรื่องค่าจ้างและอื่นๆ เพื่อจูงใจให้เจ้าหน้าที่ทำงานได้นานๆ
5.	ยังมีอีกหลายอาคารที่มีเครื่องคอมพิวเตอร์ติดไวรัส สำนักคอมพิวเตอร์ไม่มีกำลังคนที่จะเข้าไปดำเนินการ	• นำเสนอแจ้งที่ประชุมคณะกรรมการบริหารมหาวิทยาลัยรับทราบ และให้ความสำคัญในเรื่องดังกล่าว • ทำหนังสือแจ้งทุกหน่วยงานทราบ เพื่อจะได้ตระหนักความสำคัญในการติดตั้งระบบป้องกันไวรัส และช่วยตรวจสอบเครื่องคอมพิวเตอร์ตัวเองว่ามีการติดตั้งระบบป้องกันไวรัสหรือไม่
6.	ขาดแผนปฏิบัติการในการแก้ปัญหา กรณีฉุกเฉิน เพื่อดำเนินการแก้ปัญหาได้อย่างมีระบบ และขาดเจ้าภาพในการเข้าไปดำเนินการทันที เมื่อเกิดเหตุ	ควรจัดทำแผนปฏิบัติการการแก้ปัญหา กรณีฉุกเฉิน เพื่อกำหนดขั้นตอนการทำงาน ผู้รับผิดชอบติดต่อประสานงานหน่วยงานที่เกี่ยวข้อง และการ

ลำดับ	ปัญหา และอุปสรรค	ข้อเสนอแนะ
		รายงานผลความคืบหน้าต่อผู้บริหาร และหน่วยงานที่เกี่ยวข้อง
7.	ขาดการประชาสัมพันธ์และเผยแพร่ข้อมูลข่าวสารให้ชาว มศว รับทราบ	● ควรจัดทำเว็บเพจเผยแพร่ข้อมูลข่าวสารให้ ชาว มศว รับทราบ รวมทั้ง นโยบายและมาตรการการบริหารการจัดการเกี่ยวกับเครื่องไมโครคอมพิวเตอร์ ● ระบบสารสนเทศเกี่ยวกับเครื่องคอมพิวเตอร์และการติดตามงาน
8.	ควรพัฒนาระบบฐานข้อมูลเกี่ยวกับเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ที่ได้จากการข้อมูลตรวจเช็คเครื่องคอมพิวเตอร์ประจำปี มาใช้งานให้ได้ประโยชน์	● ปรับปรุงข้อมูลเครื่องคอมพิวเตอร์ ให้เป็นปัจจุบัน โดยกำหนดนโยบายการดูแลเครื่องคอมพิวเตอร์ จะต้องผ่านการลงทะเบียนผ่านทางอินเทอร์เน็ตเท่านั้น
9.	ขาดนโยบายและมาตรการ การรักษาความมั่นคงของเครือข่าย	● ควรมีการกำหนดนโยบายและมาตรการ การรักษาความมั่นคงของเครือข่าย ให้เป็นรูปธรรม ควรกำหนดนโยบายและมาตรการดูแล/ให้บริการเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ไปพร้อมๆ กัน

การดำเนินการแต่ละอาคาร

อาคาร 19 : คณะวิทยาศาสตร์

ข้อมูลเบื้องต้น

เรื่อง	ปัญหาการใช้งานเครือข่ายบัวศรีภายในอาคาร 19
วันที่ได้รับแจ้งปัญหา	วันเสาร์ที่ 30 กรกฎาคม 2548
วันที่เริ่มเข้าดำเนินการ	วันเสาร์ที่ 30 กรกฎาคม 2548
วันที่สิ้นสุดการดำเนินการ	วันจันทร์ที่ 8 สิงหาคม 2548
ระยะเวลาการดำเนินการ	10 วัน
ฝ่ายที่รับผิดชอบ	ฝ่ายปฏิบัติการและบริการ และฝ่ายระบบคอมพิวเตอร์และเครือข่าย
ผู้รับผิดชอบ	• นายวิโรจน์ เตี๋ยอนุกูล • นายถาวร หงษ์ทอง • นายสุนทร แจ่มเมือง • นายสันติ สุขยานันท์ • นายชัยวัฒน์ ช่างกลึง • นายประกิจ ลีลาเชี่ยวชาญกุล • นายไพโรจน์ ผาสุวรรณ์ (ประสานงานรับเรื่องปัญหา)

กิจกรรมดำเนินการ

วัน เดือน ปี	เวลา	กิจกรรม	เจ้าหน้าที่ดำเนินการ	ผลการดำเนินการ
ส 30 ก.ค.48	-	ได้รับแจ้งจากผู้ใช้งานคอมพิวเตอร์ไม่สามารถใช้งานเครือข่ายและอินเทอร์เน็ตภายในอาคาร 19	ประกิจ	อุปกรณ์หลักประจำอาคารใช้งานไม่ได้
ส 30 ก.ค.48	-	คุณประกิจ ได้ประสานงานกับเจ้าหน้าที่ของคณะวิทยาศาสตร์ ให้ทำการปิดและเปิดอุปกรณ์หลัก (Router) แต่อุปกรณ์หลักยังไม่สามารถใช้งานได้	ประกิจ	อุปกรณ์หลักประจำอาคารใช้งานไม่ได้
จ 1 ส.ค.48	8.30 น.	สำนักคอมพิวเตอร์ส่งเจ้าหน้าที่เข้าไปดำเนินการดังนี้ ● ทำการปิดและเปิด อุปกรณ์หลัก(Router) ประจำอาคาร อีกครั้ง และพบว่าสามารถใช้งานได้ประมาณ 15 นาที และไม่สามารถตรวจสอบได้ว่าเครื่องไมโครคอมพิวเตอร์เครื่องใดติดไวรัส ● ดังนั้นเจ้าหน้าที่สำนักคอมพิวเตอร์ทำการตรวจเช็คเครื่องไมโครคอมพิวเตอร์ทุกเครื่องภายในอาคาร หากพบเครื่องไมโครคอมพิวเตอร์ที่ไม่ได้ติดตั้งระบบป้องกันไวรัสจะดำเนินการติดตั้งระบบป้องกันไวรัสทันที	ถาวร, สุนทร, ชัยวัฒน์, สันติ, วิโรจน์, ประกิจ	อุปกรณ์หลักประจำอาคารใช้งานไม่ได้
อ. 2 ส.ค.48	8.30 น.	เจ้าหน้าที่สำนักคอมพิวเตอร์ เข้าไปดำเนินการต่อ และได้วางแผนการทำงานดังนี้ ● ตรวจสอบทีละ segment เริ่มที่สำนักงานคณบดี ชั้น 17, … ● <u>ทีมที่ 1</u> : ติดตั้งระบบตรวจจับไวรัส (sniffer) ชั่วคราว ใน segment นั้น เพื่อหาเครื่องคอมพิวเตอร์ที่ติดไวรัส ● <u>ทีมที่ 2</u> : ตรวจสอบเครื่องคอมพิวเตอร์ ทุกเครื่อง	ถาวร, สุนทร, ชัยวัฒน์, สันติ, วิโรจน์, ประกิจ	● ตรวจพบเครื่องคอมพิวเตอร์ติดไวรัส 20 เครื่อง จาก 34 เครื่อง (ชั้น 1,3) ● เครื่องคอมพิวเตอร์ของคณบดี และเจ้าหน้าที่ ชั้น 1 ควรติดตั้ง Activate Windows XP ● เครื่องคอมพิวเตอร์ของรองคณบดี (อ.ภัทณียา) อาจจะต้อง Format เครื่องใหม่

วัน เดือน ปี	เวลา	กิจกรรม	เจ้าหน้าที่ดำเนินการ	ผลการดำเนินการ
		ใน segment นั้น หากพบเครื่องไมโครคอมพิวเตอร์ที่ไม่ได้ติดตั้งระบบป้องกันไวรัสจะดำเนินการติดตั้งระบบป้องกันไวรัสทันที		
พ. 3 ส.ค.48	8.30 น.	เข้าดำเนินการตรวจเช็คเครื่องคอมพิวเตอร์ ชั้น 17	ถาวร, สุนทร, ชัยวัฒน์, สันติ, วิโรจน์, ประกิจ	• ตรวจพบเครื่องคอมพิวเตอร์ติดไวรัส 5 เครื่อง จาก 25 เครื่อง (ชั้น 17)
พฤ 4 ส.ค.48	8.30 น.	เข้าดำเนินการตรวจเช็คเครื่องคอมพิวเตอร์ ชั้น 17, 18	ถาวร, สุนทร, ชัยวัฒน์, ประกิจ	• ตรวจพบเครื่องคอมพิวเตอร์ติดไวรัส 23 เครื่อง จาก 71 เครื่อง (ชั้น 17, 18)
ศ 5 ส.ค.48	8.30 น.	เข้าดำเนินการตรวจเช็คเครื่องคอมพิวเตอร์ ชั้น 18	ถาวร, สุนทร, ชัยวัฒน์, ประกิจ	• ตรวจพบเครื่องคอมพิวเตอร์ติดไวรัส 18 เครื่อง จาก 47 เครื่อง (ชั้น 18) • เชื่อมต่ออุปกรณ์หลักระหว่างชั้น (Uplink) เข้ากับ Router แล้ว สามารถใช้งานได้ตามปกติ • ชั้น 15 ห้อง 1504 มีเครื่องคอมพิวเตอร์ 21 เครื่อง เจ้าหน้าที่แจ้งว่ายังไม่ต้องดำเนินการ เนื่องจากติดตั้งโปรแกรม GoBack ไว้ **ข้อแนะนำ** : **โปรแกรม GoBack** เป็นโปรแกรมที่ทำหน้าที่เหมือนกับ Undo Card เมื่อติดตั้งโปรแกรมใดๆ ไปแล้ว เมื่อทำการ Restart เครื่อง แล้ว Window จะกลับมาเหมือนเดิม คือเหมือนไม่ได้ติดตั้งอะไรเลย ดังนั้นจึงไม่แนะนำให้ใช้ โปรแกรมนี้กับเครื่องที่มีการเชื่อมต่อกับระบบเครือข่ายมหาวิทยาลัย

ผลการดำเนินการ

วัน เดือน ปี เข้าดำเนินการ	ชั้น	จำนวนเครื่องคอมพิวเตอร์ ตรวจสอบ		จำนวน เจ้าหน้าที่ ดำเนินการ	หมายเหตุ
		ทั้งหมด	ติดไวรัส		
2 ส.ค.48	1, 3	34	20	6	
3 ส.ค.48	17	25	5	4	
4 ส.ค.48	17, 18	71	23	4	
5 ส.ค. 48	18	47	18	4	
	รวม	130	66		

อาคารคณะวิศวะ/อาคารภาควิชาวิศวฯ โยธา : คณะวิศวกรรมศาสตร์

ข้อมูลเบื้องต้น

เรื่อง	ปัญหาการใช้งานเครือข่ายบัวศรีภายในอาคารคณะวิศวกรรมศาสตร์และภาควิชาวิศวกรรมโยธา
วันที่ได้รับแจ้งปัญหา	วันที่ 4 สิงหาคม 2548
วันที่เริ่มเข้าดำเนินการ	วันที่ 4 สิงหาคม 2548
วันที่สิ้นสุดการดำเนินการ	วันที่ 10 สิงหาคม 2548
ระยะเวลาการดำเนินการ	7 วัน
ฝ่ายที่รับผิดชอบ	ฝ่ายปฏิบัติการและบริการ
ผู้รับผิดชอบ	• นายสมเกียรติ อินตาสาย

กิจกรรมดำเนินการ

วัน เดือน ปี	เวลา	กิจกรรม	เจ้าหน้าที่ดำเนินการ	ผลการดำเนินการ
4 ส.ค. 48	10.00 น.	ได้รับแจ้งจากผู้ใช้งานคอมพิวเตอร์ไม่สามารถใช้งานเครือข่ายและอินเทอร์เน็ตภายในอาคารคณะวิศวกรรมศาสตร์ และอาคารภาควิชาวิศวกรรมโยธา	สมเกียรติ	
4 ส.ค. 48	10.00 น.	ตรวจเช็ค uplink ที่อุปกรณ์ ของสำนักคอมพิวเตอร์ และเข้าไปดำเนินการตรวจสอบอุปกรณ์เชื่อมต่อเครือข่ายย่อยที่คณะวิศวกรรมศาสตร์ ปรากฏว่าอุปกรณ์แสดงสถานะปกติ แต่ไม่สามารถใช้อินเทอร์เน็ตได้ และเป็นข้อสังเกตุว่าการ์ดแลนทำงานผิดปกติในเรื่องการ Receive packet มีมากเกินความจำเป็น สรุปว่าอาจจะเป็นปัญหาไวรัส Broadcast packet ทำให้เกิดอาการอาการ buffer overflow ที่อุปกรณ์ Switching จึงทำให้ไม่สามารถใช้งานเครือข่ายบัวศรีได้	สมเกียรติ	

วัน เดือน ปี	เวลา	กิจกรรม	เจ้าหน้าที่ดำเนินการ	ผลการดำเนินการ
4 ส.ค. 48	13.00 น.	เข้าไปดำเนินการปิดอุปกรณ์เครือข่าย และทำการตรวจสอบเครื่อง Client พบว่า มีการใช้ OS หลากหลาย Platform และยังพบว่าบางเครื่องได้ใช้ OS WIN XP แต่ยังไม่ได้ Update SP2 และ patch แก้ไข และบางเครื่องลง IE 5.0 และยังไม่ได้ upgrade ไปเป็น IE 6.0 SP 2 จึงได้ประสานงาน คุณณัฐกาญน์ เจ้าหน้าที่ของคณะดำเนินการต่อโดยดึงสายของเครื่องคอมพิวเตอร์ที่มีปัญหาออกไว้ก่อน และดำเนินการแก้ไข	สมเกียรติ	
5 ส.ค. 48	9.30 น. – 18.30 น.	• เข้าไปดำเนินการแก้ไข โดยลง patch แก้ไขKB ของไมโครซอฟท์ และติดตั้งโปรแกรม Ewido anti spyware , Hijackthis, และ Microsoft Anti Spyware และ officescan เป็นจำนวน 26 เครื่อง (เฉพาะอาคารคณะวิศวกรรมศาสตร์) • สำหรับอาคารภาควิชาวิศวกรรมโยธา จะได้เข้าไปดำเนินการในวันอังคารที่ 9 ส.ค. 48 อีกครั้ง แต่เบื้องต้นได้ ปิดอุปกรณ์ Media access converter ของอาคารภาควิชาวิศวกรรมโยธาไว้ก่อน และในส่วนของของ Access Point ซึ่งให้ใช้บริการ Wireless Lan ก็ได้ปิดบริการไว้ชั่วคราว โดยประสานงานกับเจ้าหน้าที่ภาควิชาวิศวกรรมโยธาไว้ คือคุณอนันทรัตน์ และได้บอกวิธีการแก้ไขเบื้องต้นไป • จากนั้นเวลา 13.30 ได้ไปพบคุณดิเรกและบริษัท	สมเกียรติ/ ภายในคณะวิศวกรรมศาสตร์ได้เปิดให้บริการ Wireless Lan โดยติดตั้ง Access Point ไว้จำนวน 3 ชุด / ภาควิชาวิศวกรรมโยธา ได้เชื่อมต่อจุด จากอุปกรณ์ของอาคารคณะวิศวกรรม ไปใช้งานโดยผ่าน Media access converter	

วัน เดือน ปี	เวลา	กิจกรรม	เจ้าหน้าที่ดำเนินการ	ผลการดำเนินการ
		ต่างๆ ที่เข้ามาสำรวจการเชื่อมต่อจุดเครือข่ายสำหรับห้องประชุมผู้บริหาร ชั้น 2 อาคารอำนวยการ (อันนี้ไม่เกี่ยวกับไวรัส) ● จากนั้นในเวลา 17.50 น. ได้ทำการ Up Switching อีกครั้งเพื่อทดสอบการใช้งานหลังจากที่ได้แก้ไขไปแล้วบางส่วน ผลปรากฏว่าสามารถใช้งานเครือข่ายบัวศรีได้ตามปกติหลังจากแก้ไขไปแล้ว		
6 ส.ค. 48	8.30-16.30	อยู่เวรเคาน์เตอร์ให้บริการนิสิตห้อง LAB	สมเกียรติ	
7 ส.ค. 48	8.30-16.30	อยู่เวรเคาน์เตอร์ให้บริการนิสิตห้อง LAB	สมเกียรติ	
8 ส.ค. 48	9.00-12.00	วิทยากรการใช้งาน MS-Powerpoint Basic	สมเกียรติ	
8 ส.ค. 48	13.00-16.00	วิทยากรการใช้งาน MS-Powerpoint Advance	สมเกียรติ	
9 ส.ค. 48	8.30 – 16.00	ประสานงานดำเนินการให้อาคารภาควิชาวิศวกรรมโยธา และในส่วนของการให้บริการผ่าน Access Point จะได้ประสานงานในเรื่องนโยบาย และการกำหนดสิทธิ์การเข้าใช้งานต่อไป	สมเกียรติ	ตรวจสอบคอมพิวเตอร์ 8 เครื่อง ไม่พบไวรัสแต่ได้ Update patch แก้ไขเพิ่มเติม
10 ส.ค. 48	8.30 – 10.00	วิเคราะห์ถึงสาเหตุที่เครื่อง Client ของภาควิชาโยธาไม่ได้รับ IP Address สรุปว่าสาย UTP เสีย แก้ไขโดยเปลี่ยนสาย UTP ที่ Link ของ Media Access Converter จึงทำให้ใช้งานได้โดยปกติ	สมเกียรติ	เครือข่ายภายในอาคารภาควิชาวิศวฯ โยธา ใช้งานได้ตามปกติ

ผลการดำเนินการ

วัน เดือน ปี เข้าดำเนินการ	ชั้น	จำนวนเครื่องคอมพิวเตอร์ ตรวจสอบ		จำนวน เจ้าหน้าที่ ดำเนินการ	หมายเหตุ
		ทั้งหมด	ติดไวรัส		
5 ส.ค.48	1, 2	36	36	1	อาคารคณะวิศวกรรมศาสตร์
9 ส.ค. 48	2, 3	8	0	1	อาคารภาควิชาวิศวกรรมโยธา
	รวม	44	36		

อาคารสมเด็จพระเทพฯ : สำนักหอสมุดกลาง

ข้อมูลเบื้องต้น

เรื่อง	ปัญหาการใช้งานระบบห้องสมุดได้บ้างไม่ได้บ้าง เช่น ระบบงานยืม-คืน ระบบ Search ข้อมูลห้องสมุด ใช้ได้ประมาณครึ่งชั่วโมง ก็ไม่สามารถใช้งานต่อได้ จะต้อง restart เครื่องคอมพิวเตอร์ลูกข่าย (Client) ก็สามารถใช้งานได้ตามปกติ
วันที่ได้รับแจ้งปัญหา	4 สิงหาคม 2548
วันที่เริ่มเข้าดำเนินการ	4 สิงหาคม 2548
วันที่สิ้นสุดการดำเนินการ	8 สิงหาคม 2548
ระยะเวลาการดำเนินการ	4 วัน
ฝ่ายที่รับผิดชอบ	ฝ่ายระบบคอมพิวเตอร์และเครือข่าย
ผู้รับผิดชอบ	• นายมหัทธวัฒน์ รักษาเกียรติศักดิ์ • นายนคร บริพนธ์มงคล • นายประกิจ ลีลาเชี่ยวชาญกุล

กิจกรรมดำเนินการ

วัน เดือน ปี	เวลา	กิจกรรม	เจ้าหน้าที่ดำเนินการ	ผลการดำเนินการ
พฤ 4 ส.ค.48	10.00 น.	เจ้าหน้าที่สำนักหอสมุดกลางแจ้งว่าการใช้งานเครือข่ายไม่ได้	มหัทธวัฒน์, ประกิจ	แนะนำให้ตรวจสอบเกี่ยวกับเรื่องการติดไวรัส ก่อน เนื่องจากช่วงเวลาดังกล่าว มีปัญหาการระบาดไวรัสภายใน มศว อยู่ พบว่า
ศ 5 ส.ค.48	9.00 น.	สำนักคอมพิวเตอร์ส่งเจ้าหน้าที่เข้าไปตรวจสอบสาเหตุ	มหัทธวัฒน์ , นคร	• ตรวจสอบอุปกรณ์หลักประจำอาคาร ไม่พบปัญหา • จากการสังเกตุ ระบบห้องสมุดใช้งานได้เป็นช่วงๆ ประมาณครึ่งชั่วโมง หากใช้งานไม่ได้ จะต้อง restart เครื่องคอมพิวเตอร์ลูกข่าย (Client) จึงจะทำงานได้ตามปกติ ☐ เจ้าหน้าที่สำนักหอสมุดกลางติดต่อประสานงานกับบริษัทผู้

วัน เดือน ปี	เวลา	กิจกรรม	เจ้าหน้าที่ดำเนินการ	ผลการดำเนินการ
				ติดตั้งระบบห้องสมุด เพื่อเข้ามาตรวจสอบระบบในวันจันทร์ 8 ส.ค.48
จ 8 ส.ค.48	13.30	บริษัทเข้ามาตรวจสอบระบบห้องสมุด	บริษัทติดตั้งระบบห้องสมุด, มหัทธวัฒน์	ระบบห้องสมุดใช้งานได้ตามปกติ แต่ยังไม่ทราบสาเหตุที่ชัดเจน จึงเห็นควรให้สำนักหอสมุดกลางนัดผู้เกี่ยวข้อง (เจ้าหน้าที่สำนักหอสมุดกลาง เจ้าหน้าที่สำนักคอมพิวเตอร์ และบริษัทดูแลระบบห้องสมุด) ร่วมกันสรุปประเด็นและสาเหตุที่เกิดขึ้นต่อไป

ผลการดำเนินการ

ระยะเริ่มแรกได้เข้าไปตรวจสอบอุปกรณ์หลักประจำอาคาร ไม่พบปัญหา จากการสังเกตุ ระบบห้องสมุดใช้งานได้เป็นช่วงๆ ประมาณครึ่งชั่วโมง หากใช้งานไม่ได้ จะต้อง restart เครื่องคอมพิวเตอร์ลูกข่าย (Client) จึงจะทำงานได้ตามปกติ และได้ประสานงานกับบริษัทติดตั้งระบบห้องสมุดมาตรวจสอบระบบห้องสมุด ขณะนี้ระบบห้องสมุดใช้งานได้ตามปกติ แต่ยังไม่ทราบสาเหตุที่ชัดเจน จึงเห็นควรให้สำนักหอสมุดกลางนัดผู้เกี่ยวข้อง (เจ้าหน้าที่สำนักหอสมุดกลาง เจ้าหน้าที่สำนักคอมพิวเตอร์ และบริษัทดูแลระบบห้องสมุด) ร่วมกันสรุปประเด็นและสาเหตุที่เกิดขึ้นต่อไป

คณะผู้จัดทำเอกสาร

1. นายดิเรก อึ้งตระกูล
2. นายมหัทธวัฒน์ รักษาเกียรติศักดิ์
3. นายวิโรจน์ เตี๋ยอนุกูล
4. นายสมเกียรติ อินตาสาย
5. นายสมบุญ อุดมพรยิ่ง

แฟ้มข้อมูล : virus2548_0708r.doc