หนอนอินเทอร์เน็ต W32.Nachi.Worm กับระบบเครือข่ายภายใน ร.ร.นร

น.ต.ไกรสิทธิ์ มหิวรรณ
อาจารย์ฝ่ายศึกษา

เช้าวันที่ ๑๘ สิงหาคม ๒๕๔๖ เวลา ๐๕๓๐ (ตามเวลา U.S. Pacific Time) หรือเวลาประมาณ ๑๗๓๐ ของวันเดียวกันตามเวลาท้องถิ่นในประเทศไทย ได้มีรายงานการแพร่ระบาดของหนอนอินเทอร์เน็ตในประเทศญี่ปุ่น ไต้หวัน และสิงค์โปร์ หนอนอินเทอร์เน็ตตัวนี้มีชื่อว่า **WORM_MSBLAST.D** และมีชื่ออื่น ๆ อีกคือ **W32.Welchia.Worm, W32.Nachi.worm, Win32.Nachi.Worm, Welchia, W32/Nachi-A** ซึ่งเป็นคนละชนิดกับ **W32.Blaster.Worm** ตามที่ได้มีการเผยแพร่ข่าวเรื่องการระบาดของหนอนอินเทอร์เน็ตตามสื่อต่าง ๆ มากมายทั่วประเทศ หนอนอินเทอร์เน็ตชนิดนี้จะมีผลกระทบต่อเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการวินโดว์เอ็กซ์พี และวินโดว์ 2000 (Windows XP, 2000) คล้าย ๆ กับ **W32.Blaster.Worm** โดยอาศัยช่องโหว่บนระบบปฏิบัติการทำให้เครื่องที่โดนเล่นงานกลายเป็นแหล่งดาวน์โหลดหนอนชนิดนี้ หลังจากนั้นจะเข้าควบคุมเครื่องอื่นให้เข้ามาดาวน์โหลด และจะเริ่มการทำงานทุกครั้งที่เปิดเครื่อง นอกจากนั้นหนอนชนิดนี้ยังพยายามที่จะกำจัดหนอน **W32.Blaster.Worm** ออกไปจากเครื่องคอมพิวเตอร์ที่ถูกเล่นงานด้วย

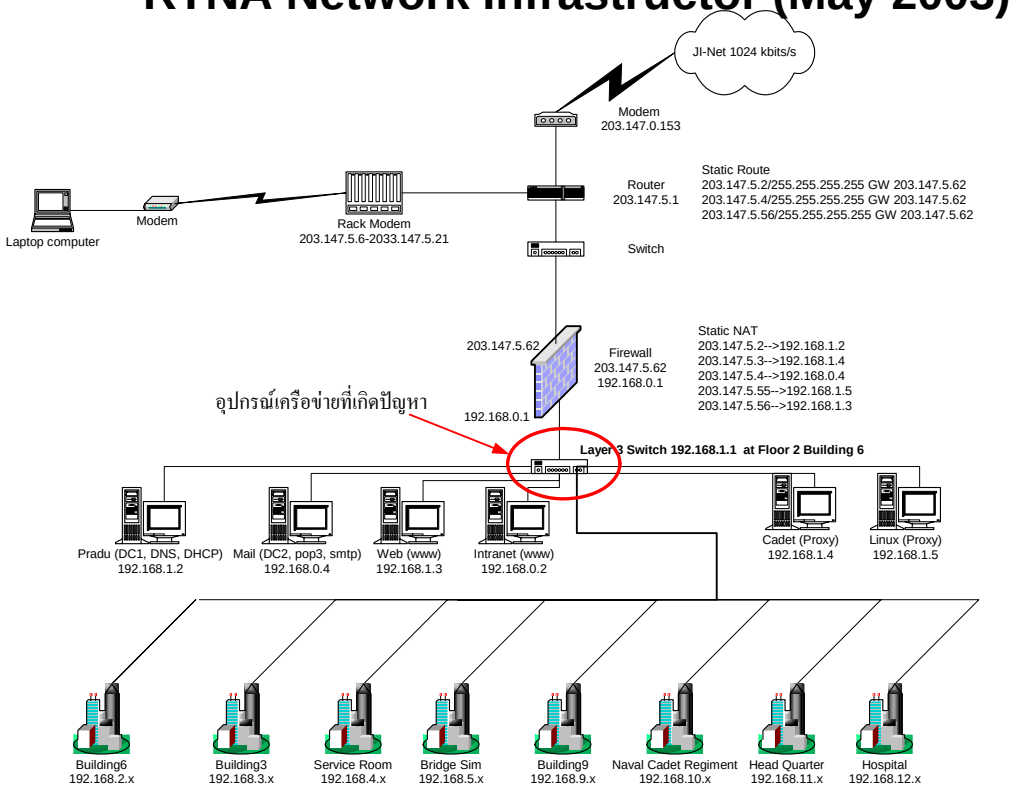
การแพร่กระจายของหนอน Win32.Nachi.Worm

การแพร่กระจายของหนอนตัวนี้จะดำเนินการโดยเครื่องที่โดนเล่นงานจะสแกนเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในระบบเครือข่ายทุกเครื่องที่เปิดพอร์ท **135/TCP** ไว้เพื่อดูว่าจะสามารถนำหนอนไปแพร่ได้หรือไม่ เมื่อเจอเป้าหมายก็จะสั่งการให้เครื่องเป้าหมายเข้ามาดาวน์โหลดหนอนไปจากเครื่องที่โดนเล่นงานก่อนแล้วโดยอาศัยช่องสัญญาณที่ ๖๖๖ ถึง ๗๖๕ **(port:666-675)** เมื่อเครื่อง เป้าหมายโดนเล่นงานก็จะมีอาการเช่นเดียวกับเครื่องที่ติดหนอนชนิดนี้เครื่องอื่น ๆ คือทำให้ตัวเองเป็นแหล่งดาวน์โหลดและสแกนระบบเครือข่ายเพื่อนำไปติดเครื่องอื่น ๆ และผลจากการสแกนและส่งแพ็คเกจ อย่างหนักในระบบเครือข่ายจากการกระทำของหนอนชนิดนี้ทำให้ระบบเครือข่ายเกิดความเสียหายไม่สามารถใช้การได้

ผลกระทบต่อระบบเครือข่ายโรงเรียนนายเรือ

เนื่องจากระบบเครือข่ายโรงเรียนนายเรือ ได้ดำเนินการติดตั้งกำแพงไฟ (Firewall) เพื่อการรักษาความปลอดภัยให้แก่ระบบ จากเหตุการณ์การแพร่กระจายของหนอนชนิดนี้ในวันที่ ๑๘ สิงหาคม ๒๕๔๖ ไม่ส่งผลกระทบต่อระบบเครือข่ายโรงเรียนนายเรือ เพราะ**พอร์ทที่ ๑๓๕ และ ๖๖๖ ถึง ๗๖๕ ได้ถูกปิด**

จากการเชื่อมต่อกับระบบเครือข่ายภายนอกไว้แล้วโดยกำแพงไฟจึงทำให้ระบบเครือข่ายภายในโรงเรียนนายเรือ ปลอดภัยจากหนอนชนิดนี้ได้ในเบื้องต้น



รูปที่ ๑

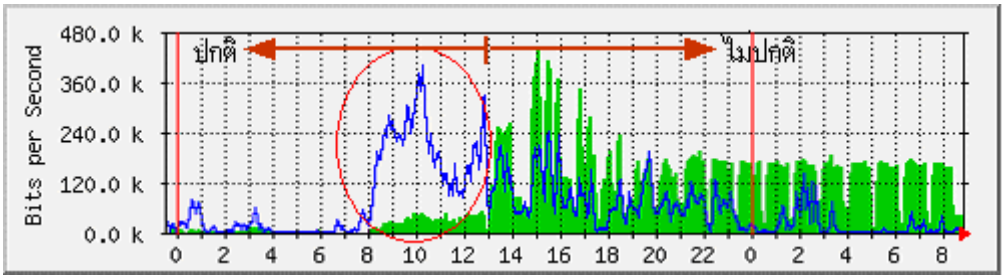
ในวันพุธที่ ๔ กันยายน ๒๕๔๖ เวลาประมาณ ๑๒๓๐ ระบบเครือข่ายโรงเรียนนายเรือ ได้เริ่มเกิดปัญหาในการใช้งานขึ้นโดยมีอาการใช้งานได้บ้างไม่ได้บ้างเป็นจังหวะ โดยผู้เขียนเข้าใจว่าปัญหาดังกล่าวได้เกิดขึ้นเฉพาะเครื่องคอมพิวเตอร์ของผู้เขียนเองเพราะได้กำลังทดลองใช้งานเครื่องคอมพิวเตอร์อีกเครื่องที่ไม่ค่อยจะสมบูรณ์และไม่นานนักก็ได้รับแจ้งจากบริเวณข้างเคียงว่าเกิดปัญหาเดียวกันนี้บนเครื่องคอมพิวเตอร์เครื่องอื่นอีก จึงได้เริ่มทำการตรวจสอบ โดยเริ่มตรวจสอบที่อุปกรณ์เครือข่าย (Layer III Switch) ที่ชั้น ๒ ของอาคารกองวิชาวิศวกรรมเครื่องกลเรือ (รูปที่ ๑ ที่ลูกศรชี้) พบว่ามีการทำงานอย่างผิดปกติคืออุปกรณ์ตัวนี้ได้มีการปิดตัวเองและเริ่มทำงานใหม่อัตโนมัติบ่อยครั้งมากและระบบเครือข่ายจะใช้งานได้ในช่วงที่อุปกรณ์นี้เริ่มทำงานในไม่กี่นาทีแรกเท่านั้นหลังจากนั้นจะใช้งานไม่ได้และอุปกรณ์ตัวนี้ก็จะรี-สตาร์ทตัวเองและวนเวียนลักษณะนี้ตลอด

จากการตรวจสอบพอร์ทที่เชื่อมต่อกับอาคารต่าง ๆ ในโรงเรียนนายเรือ บนอุปกรณ์นี้จึงเห็นว่ามีการส่งข้อมูลเข้ามาที่บางพอร์ทมากอย่าง ผิดปกติจึงเป็นสาเหตุให้อุปกรณ์ตัวนี้ทำงานไม่ไหวจึงหยุดการทำงานและต้องรี-สตาร์ทตัวเองอัตโนมัติซึ่งเป็นสาเหตุให้ระบบเครือข่ายใช้งานได้บ้างไม่ได้บ้าง เมื่อตรวจสอบข้อมูลบนเครื่องคอมพิวเตอร์ ที่ทำหน้าที่เป็นกำแพงไฟก็ไม่พบสิ่งปกติใด ๆ แต่เมื่อตรวจสอบข้อมูลที่บันทึกการทำงานของเครื่องเซิร์ฟเวอร์ ก็พบว่ามีไวรัสชนิดหนึ่งเข้ามาอยู่ในเครื่องคอมพิวเตอร์และได้ถูกกำจัดออกไปแล้วโดยโปรแกรมป้องกันไวรัสบนเครื่อง เมื่อพิจารณารายละเอียดข้อมูลของไวรัสจึงได้ทราบว่าเป็นหนอนอินเทอร์เน็ตชนิดหนึ่งที่มีชื่อว่า **WORM_MSBLAST.D** หรือ **W32.Nachi.Worm** แสดงว่าหนอนชนิดนี้ได้มีการเล็ดลอดเข้ามาในระบบเครือข่ายของโรงเรียนนายเรือและน่าจะเป็นสาเหตุของความผิดปกติของระบบเครือข่าย จึงได้ทำการปลดการเชื่อมต่อเข้ากับอุปกรณ์เครือข่าย (Layer III Switch) ของอาคารต่าง ๆ ที่ทำให้อุปกรณ์ตัวนี้เกิดปัญหาซึ่งได้แก่ อาคาร ๓ อาคาร ๙ อาคารกองบัญชาการ และอาคารฝึกจำลองเรือเดิน (Bridge Sim) จึงทำให้ระบบที่เหลือซึ่งได้แก่ อาคาร ๔ - ๕ อาคาร๖และโรงพยาบาลโรงเรียนนายเรือเข้าสู่สภาวะการทำงานอย่างปกติในเช้าวันพฤหัสที่ ๕ กันยายน ๒๕๔๖ และเป็นเวลาทั้งสิ้น ๑๗ วันนับจาก วันที่หนอนชนิดนี้ได้เริ่มระบาดในระบบเครือข่ายต่าง ๆ ทั่วโลก

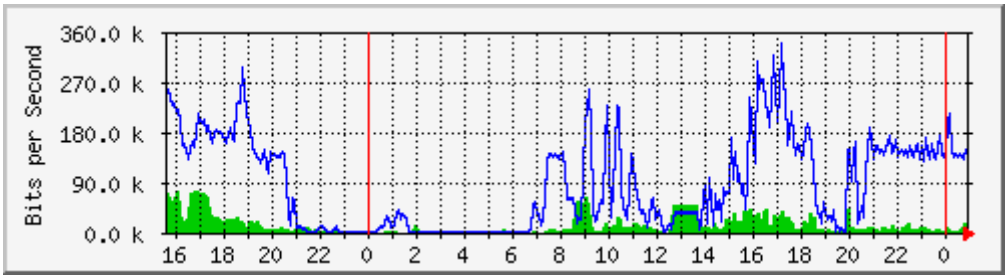
เครื่องมือที่ช่วยในการวิเคราะห์ปัญหา

หลังจากที่ได้ทราบข้อมูลและมีความเป็นไปได้ว่าหนอน **WORM_MSBLAST.D** ได้แพร่ระบาดในระบบเครือข่ายของโรงเรียนนายเรือ และในเบื้องต้นได้สังเกตการณ์ทำงานของ Layer III Switch พบว่าบางพอร์ทมีการส่งข้อมูลออกมากอย่างผิดปกติและได้ทำการปลดการเชื่อมต่อของบางอาคารออกจากระบบเครือข่ายหลักไปแล้วนั้น ก็ได้ดำเนินการตรวจสอบสถิติปริมาณของข้อมูลที่ผ่านเข้า-ออกแต่ละพอร์ทบน Layer III Switch โดยดูจากกราฟที่ได้ทำการบันทึกสถิติไว้ทุก ๕ นาทีโดยโปรแกรมที่ชื่อว่า MRTG (Multi Router Traffic Router) ซึ่งได้นำมาติดตั้งบนเครื่องเซิร์ฟเวอร์ของกองวิชาวิศวกรรมเครื่องกลเรือ (กววร.ฯ) เพื่อใช้ตรวจสอบการใช้งานระบบเครือข่ายภายในโรงเรียนนายเรือ หลายเดือนที่แล้ว จากการพิจารณากราฟที่ได้ก็พบความผิดปกติของข้อมูลที่เข้า-ออกในแต่ละพอร์ทที่มีปัญหาเช่น ในรูปที่ ๒ ซึ่งเป็นกราฟแสดงข้อมูลเข้า-ออกของพอร์ทที่เชื่อมต่อกับเราท์เตอร์มีข้อมูลขาออก(ส่งออกไปข้างนอกเครือข่าย)มากผิดปกติตั้งแต่เวลาประมาณ ๑๓๐๐ ของวันที่ ๔ กันยายน ๒๕๔๖ เส้นกราฟที่แสดงเป็นเส้นเดี่ยวคือปริมาณข้อมูลขาเข้ามายังภายในซึ่งปกติจะมีมากกว่าข้อมูลขาออก ส่วนเส้นกราฟทึบ จะแสดงปริมาณข้อมูลขาออกไปยังเครือข่ายภายนอกซึ่งปกติจะไม่สูงมากนักและน้อยกว่าข้อมูลขาเข้า สังเกตุได้ว่าในช่วงเวลา ๐๘๐๐ ถึง ๑๓๐๐ (ในวงกลม) ระบบเครือข่ายยังทำงานปกติ ในรูปที่ ๓ เป็นตัวอย่างของกราฟในช่วงการทำงานอย่างปกติของพอร์ทเดียวกันหลังจากที่ได้แก้ไขปัญหาแล้ว ในรูปที่ ๔ เป็นกราฟของข้อมูลที่เข้า-ออกของอาคารหลังหนึ่งที่มีปัญหาการระบาดของหนอนชนิดนี้ จะเห็นได้ว่าในช่วงเวลาประมาณ ๑๓๐๐ ถึง ๑๗๐๐ มีข้อมูลถูกส่งออกจากอาคารนั้นเป็นจำนวนมากผิดปกติและส่งผลให้ระบบ

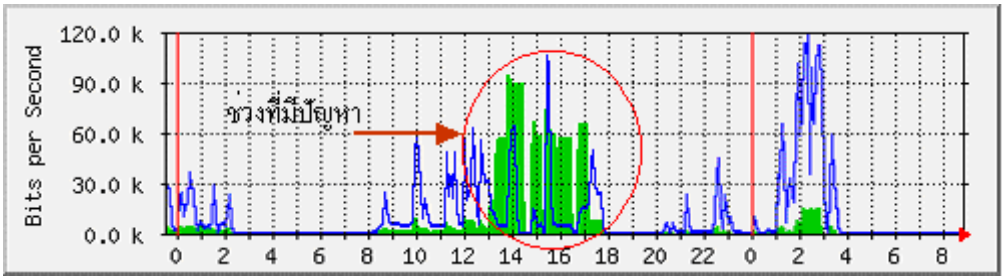
เครือข่ายหลักมีปัญหา จึงต้องทำการปลดการเชื่อมต่อของอาคารหลังนี้ออกจากระบบเครือข่ายหลักเพื่อให้ระบบโดยรวมสามารถใช้งานได้อย่างปกติ



รูปที่ ๒



รูปที่ ๓



รูปที่ ๔

เครื่องมืออีกอย่างในการนำมาใช้เพื่อช่วยตรวจสอบว่าเครื่องคอมพิวเตอร์เครื่องใดใช้ระบบปฏิบัติการ Windows XP/ 2000 โดยที่ยังไม่ได้ติดตั้งโปรแกรมแก้ไขข้อบกพร่องก็คือโปรแกรม DCOM-KB826369-X86-ENU.exe ที่บริษัทไมโครซอฟท์ ได้พัฒนาขึ้นมาเพื่อให้ผู้ดูแลระบบใช้ร่วมในการช่วย แก้ไขปัญหาที่เกิดจากหนอนชนิดนี้ได้สะดวกขึ้น ทำให้ทราบว่าเครื่องคอมพิวเตอร์เครื่องใด ไอพีแอดเดรส ใดที่มีโอกาสถูกโจมตีจากหนอนตัวนี้บ้าง

การดำเนินการแก้ไข

ได้เริ่มดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ที่อาคารต่าง ๆ ที่มีปัญหาการระบาดของหนอนอินเทอร์เน็ต โดยเริ่มที่อาคารกองวิชาวิศวกรรมศาสตร์เนื่องจากมีข้อมูลที่ชัดเจนว่ามีเครื่องคอมพิวเตอร์เครื่องใดที่ใช้ระบบปฏิบัติการ Windows XP และ 2000 จากการตรวจสอบพบหนอน **WORM_MSBLAST.D** บนเครื่องคอมพิวเตอร์จำนวน ๑ เครื่องจึงดำเนินการแก้ไขโดยนำโปรแกรมสแกนไวรัสที่ออกมาล่าสุดไปสแกนเพื่อกำจัดหนอนชนิดนี้ออกจากเครื่องคอมพิวเตอร์จากนั้นได้นำโปรแกรมสำหรับการอุดช่องโหว่หรือข้อบกพร่องของระบบปฏิบัติการไปติดตั้งเพิ่มเติมเพื่อไม่ให้เครื่องคอมพิวเตอร์ถูกโจมตีจากหนอนชนิดนี้อีกเมื่อแก้ไขเรียบร้อยจึงได้ทำการเชื่อมต่อระบบของอาคารกองวิชาวิศวกรรมศาสตร์เข้ากับระบบเครือข่ายหลักและสามารถใช้งานได้อย่างปกติ ซึ่งเป็นเครื่องยืนยันว่าปัญหาของระบบเครือข่ายเกิดจากหนอน **WORM_MSBLAST.D** หลังจากนั้นได้เริ่มการแก้ไขที่อาคารต่าง ๆ โดยตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่ใช้ระบบปฏิบัติการ Windows XP และ 2000 และได้ตรวจสอบไวรัสชนิดอื่นบนเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Windows 98 และ ME บางเครื่องที่มีโอกาส ปรากฏผลดังนี้

อาคาร	จำนวนเครื่องคอมพิวเตอร์ที่ตรวจพบหนอน **WORM_MSBLAST.D**
กองบัญชาการ	1
อาคาร 3	1
อาคาร 6	1
อาคาร 9	1
ห้อง Server	3
Bridge Sim	เจ้าหน้าที่ที่อาคารได้แก้ไขเองจึงไม่ได้รับรายงาน

เครื่องคอมพิวเตอร์ที่โดนหนอน **WORM_MSBLAST.D** เล่นงานได้ถูกสแกนเพื่อกำจัดหนอนและได้ติดตั้งโปรแกรมเพื่อแก้ไขข้อบกพร่องและได้ทำการเชื่อมต่อระบบเครือข่ายของอาคารต่าง ๆ เข้ากับระบบเครือข่ายหลักในวันที่ 9 กันยายน 2546 เวลาประมาณ 1300 ซึ่งระบบโดยรวมทั้งระบบทำงานได้อย่างปกติ

ปัญหาข้อขัดข้องต่าง ๆ ที่เกิดขึ้นและข้อเสนอแนะ

ระบบเครือข่ายโรงเรียนนายเรือได้ติดตั้งกำแพงไฟขึ้นมาเพื่อสร้างความปลอดภัยให้ระบบเครือข่ายได้ระดับหนึ่ง โดยเหตุการณ์ระบาดของหนอนอินเทอร์เน็ต **WORM_MSBLAST.D** นั้นการทำงานโดยทั่วไปของหนอนชนิดนี้ไม่สามารถจะเจาะทะลุผ่านกำแพงไฟเข้ามาได้จึงทำให้ปลอดภัยจากหนอนนี้ได้ใน

ตอนต้น แต่จากการระบาดของหนอนชนิดนี้ในระบบเครือข่ายแสดงว่าได้มีการนำเครื่องคอมพิวเตอร์ที่โดนหนอนชนิดนี้เล่นงานมาแล้วเข้ามาเชื่อมต่อกับระบบเครือข่ายของโรงเรียนนายเรือ ซึ่งไม่สามารถป้องกันการระบาดภายในได้ ทำให้เครื่องคอมพิวเตอร์เครื่องอื่น ๆ ภายในระบบเครือข่ายได้รับผลกระทบด้วย กำแพงไฟที่ติดตั้งสามารถป้องกันการบุกรุกจากภายนอกได้ซึ่งเป็นตัวกลางระหว่างเครือข่ายภายนอกและเครือข่ายภายใน แต่การระบาดที่เกิดขึ้นภายในเองนั้นกำแพงไฟไม่สามารถป้องกันได้ ดังนั้นความปลอดภัยของระบบเครือข่ายนอกจากจะต้องใช้กำแพงไฟแล้วจะต้องใช้วินัยในการใช้เครื่องคอมพิวเตอร์ของผู้ใช้งานทุกคนด้วย เช่น การติดตามข่าวสารบนสื่อต่าง ๆ และดำเนินการป้องกันให้แก่เครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เพื่อไม่ให้ถูกโจมตีและระบาดไปยังเครื่องอื่น ๆ การนำเครื่องคอมพิวเตอร์ชนิดพกพาได้มาเชื่อมต่อกับระบบเครือข่ายภายในโรงเรียนนายเรือ ก็จะต้องตรวจสอบเครื่องคอมพิวเตอร์ของตนเองว่าไปติดไวรัสที่ไหนมาบ้างหรือไม่ หากติดมาก็จะทำให้เครือข่ายภายในเกิดปัญหาได้ การอัพเดท ให้โปรแกรมป้องกันไวรัสบนเครื่องคอมพิวเตอร์ของตนเองอย่างสม่ำเสมอก็เป็นอีกแนวทางในการแสดงความรับผิดชอบต่อระบบโดยรวม เครื่องคอมพิวเตอร์ของผู้เขียนเองก็โดนหนอน **WORM_MSBLAST.D** โจมตีเช่นกันแต่โปรแกรมป้องกันไวรัสได้แจ้งเตือนและแก้ไขให้เนื่องจากได้ทำการอัพเดทข้อมูลเกี่ยวกับไวรัสเสมอ ในการตรวจสอบเครื่องคอมพิวเตอร์ตามอาคารต่าง ๆ ได้มีโอกาสสแกนเครื่องคอมพิวเตอร์ที่ไม่ใช่เป้าหมายในการโจมตีของหนอนชนิดนี้พบไวรัสชนิดอื่นหลายชนิดมากบนเครื่องคอมพิวเตอร์ที่ต่าง ๆ นอกจากนั้นพบว่าเครื่องคอมพิวเตอร์บางเครื่องยังไม่ได้ติดตั้งโปรแกรมป้องกันไวรัสและหลายเครื่องที่ ไม่มีการอัพเดทข้อมูลของไวรัสให้แก่โปรแกรมเหล่านี้ทำให้ไม่สามารถป้องกันไวรัสที่เกิดขึ้นใหม่ ๆ ได้ การนำโปรแกรมต่าง ๆ ที่ไม่ได้ใช้ในการปฏิบัติงานหรือเกมส์ต่าง ๆ มาติดตั้งบนเครื่องคอมพิวเตอร์ที่ ใช้งานอยู่นั้นก็เป็นอีกสาเหตุหนึ่งของปัญหาต่าง ๆ ที่เกิดขึ้นหากโปรแกรมเหล่านั้นมีไวรัสแอบแฝงอยู่ ซึ่งบางครั้งทำความเสียหายให้ระบบได้หรืออาจจะทำให้ผู้โจมตีระบบสามารถขโมยข้อมูลที่สำคัญต่าง ๆ ไปได้

ในส่วนของการแก้ไขปัญหาตามอาคารต่าง ๆ ก็มีปัญหาบ้างเล็กน้อยนั่นคือ เจ้าหน้าที่ที่ทำหน้าที่ในการดูแลระบบเครือข่ายโรงเรียนนายเรือ นั้นมีเพียง ๓ นาย ซึ่งเป็นอาจารย์ของกองวิชาวิศวกรรมศาสตร์และวิศวกรรมเครื่องกลเรือและก็มีหน้าที่ประจำในการสอนอยู่แล้วโดยเฉพาะในช่วงเวลานี้เป็นช่วงที่จะต้องทำการตรวจข้อสอบปลายภาคและเตรียมการสอนในภาคการศึกษาถัดไปทำให้ไม่สามารถดูแลและแก้ไขได้อย่างเต็มที่ จะเห็นได้ว่าในการตรวจและแก้ไขปัญหาที่เกิดขึ้นซึ่งเริ่มเกิดปัญหาในวันที่ ๔ กันยายน ๒๕๔๖ ตรวจสอบพบปัญหาและแก้ไขในเบื้องต้นได้ใน ๕ กันยายน ๒๕๔๖ แต่แก้ไขเสร็จสิ้นทำให้ทั้งระบบใช้งานได้อย่างสมบูรณ์ใน ๙ กันยายน ๒๕๔๖ ทำให้การเชื่อมต่อในบางอาคารต้องหยุดชะงักไปเป็นเวลาถึง ๕ วัน (๓ วันทำการ) หากศูนย์คอมพิวเตอร์มีเจ้าหน้าที่ประจำที่มีความรู้ความสามารถในด้านระบบเครือข่ายโดยตรงอย่างเพียงพอก็จะสามารถดำเนินการแก้ไขได้รวดเร็วกว่านี้

สรุป

จากเหตุการณ์ครั้งนี้ถึงแม้หนอน **WORM_MSBLAST.D** จะไม่ได้ทำความเสียหายต่อระบบเครือข่ายโรงเรียนนายเรือ ได้มากนักแต่ก็เป็นอุทาหรณ์ให้แก่ทุกคนได้ดีว่าการดำเนินการป้องกันให้แก่เครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่และการป้องกันให้ระบบเครือข่ายของโรงเรียนนายเรือ นั้นไม่สามารถอาศัยเฉพาะเจ้าหน้าของศูนย์คอมพิวเตอร์ได้เพียงอย่างเดียวจะต้องอาศัยความร่วมมือของทุกคนในการดำเนินการและการใช้งาน เพราะในอนาคตข้างหน้าอาจจะมีไวรัสหรือหนอนอินเทอร์เน็ตที่มีความสามารถในการทำความเสียหายแก่ระบบได้มากกว่านี้เกิดขึ้นซึ่งอาจจะถึงขั้นต้องทำให้สูญเสียข้อมูลที่สำคัญทั้งหมดไปก็เป็นไปได้และก็อาจจะต้องแก้ไขโดยการลบทุกอย่างทิ้งและเริ่มทุกอย่างใหม่หมด เช่น การสูญเสียข้อมูลงบประมาณของหน่วย ข้อมูลเงินเดือนของข้าราชการ ข้อมูลกำลังพล ถึงแม้สิ่งเหล่านี้จะสามารถนำกลับมาได้แต่ก็ได้สร้างความลำบากให้เราได้ไม่มากก็น้อย แต่หากในบางกรณีที่ข้อมูลต่าง ๆ ถูกแก้ไขโดยที่ผู้ใช้ไม่ได้ตรวจสอบและนำไปใช้งาน อาจทำความเสียหายให้แก่หน่วยได้มากกว่า สิ่งต่าง ๆ เหล่านี้คือภัยที่เกิดขึ้นอยู่ในโลกอินเทอร์เน็ตและเกี่ยวข้องกับเราโดยตรงไม่สามารถที่จะละเลยได้ การมีวินัยในการใช้ระบบเครือข่ายและการใช้เครื่องคอมพิวเตอร์ การหมั่นขยันหาข้อมูลความรู้ก้าวทันโลกติดตามเทคโนโลยีก็เป็นหนทางหนึ่งในการ ป้องกันตนเองและส่วนรวมให้ปลอดภัยจากอันตรายที่เรามองไม่เห็น

เอกสารอ้างอิง

www.thaicert.nectec.or.th

www.trendmicro.com

www.pantip.com/tech/software/

www.microsoft.com