บทที่ ๑
รู้จักเพื่อนสนิทคอมพิวเตอร์

ขอขึ้นต้นด้วยข้อความ “รู้จักเพื่อนสนิทคอมพิวเตอร์” ซึ่งในความหมายที่จะกล่าวถึงในต่อไปก็คือ โปรแกรมที่อยู่ในคอมพิวเตอร์โดยเราอาจจะรู้บ้าง หรือไม่รู้บ้าง แต่โปรแกรมพวกนี้ทำให้คอมพิวเตอร์ของผู้ใช้มีปัญหา จึงเป็นข้อความเชิงประชดขึ้นมา และโปรแกรมที่ก่อให้เกิดปัญหากับคอมพิวเตอร์นั้นผู้ใช้โดยทั่วไปมักเรียกว่า ไวรัสคอมพิวเตอร์ (Computer Viruses) เมื่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ถูกโปรแกรมจำพวกนี้เล่นงานก็จะบอกว่าโดนไวรัส ซึ่งในความเป็นจริงแล้วโปรแกรมที่ทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์มีปัญหานั้น ถ้าเรียกให้ถูกต้อง คือ Malicious Software หรือ เรียกว่า มัลแวร์ (Malware)

สาเหตุที่เรียกโปรแกรมที่สร้างความเสียหายให้กับระบบคอมพิวเตอร์ว่าไวรัส เพราะไวรัสเป็นมัลแวร์ชนิดแรกที่เกิดขึ้นและมีมานาน ดังนั้น เวลาจะกล่าวถึงเรื่องโปรแกรมที่สร้างความเสียหายให้กับระบบคอมพิวเตอร์ คนทั่วไปจึงมักเรียกว่า ไวรัส

๑. มัลแวร์ (Malware)

มัลแวร์ มาจากคำว่า Malicious Software โดยนำคำว่า Mal มาจาก Malicious และ ware มาจาก Software เป็นคำเรียกว่า Malware ซึ่งหมายถึงโปรแกรมที่ประสงค์ร้าย ที่ถูกออกแบบมาให้แทรกซึม ปั่นป่วน หรือทำความเสียหายให้กับระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์

มัลแวร์ประกอบด้วยหลายชนิด ซึ่งพอจะยกมากล่าวถึงได้ดังนี้

๑.๑ ไวรัส (Viruses)

โปรแกรมชนิดหนึ่งที่มีลักษณะหรือความสามารถในการแพร่เชื้อไปติดไฟล์อื่นๆ ในคอมพิวเตอร์ หรือผ่านระบบเครือข่ายคอมพิวเตอร์ ซึ่งการที่คอมพิวเตอร์ติดไวรัส นั้นหมายความว่า ไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำของเครื่องคอมพิวเตอร์แล้ว ส่วนจะทำงานในลักษณะเช่นใดก็ขึ้นอยู่กับผู้สร้างโปรแกรมมา โดยปกติผู้ใช้คอมพิวเตอร์จะไม่รู้ว่ามีไวรัสอยู่หรือไวรัสทำงานอยู่ จนกว่าจะแสดงอาการออกมา เช่น เครื่องคอมพิวเตอร์ทำงานช้าลง หรือค้าง เป็นต้น เราสามารถจำแนกไวรัส ได้เป็นดังนี้

๑.๑.๑ บูตเซคเตอร์ไวรัส (Boot Sector Viruses) ในเซคเตอร์แรกของฮาร์ดดิสก์จะถูกเก็บโปรแกรมส่วนที่ใช้ในระบบปฏิบัติการ (Operating System) ซึ่งจะถูกเรียกใช้โดยตัวไบออส (BIOS) เมื่อไวรัสฝังตัวอยู่ในนี้ ทุกครั้งที่บูตเครื่องคอมพิวเตอร์ขึ้นมา ตัวไวรัสก็จะทำงานทันที โดยมาฝังตัวอยู่ในหน่วยความจำ

๑.๑.๒ ไฟล์ไวรัส (File Viruses) หรือบางทีอาจจะเรียกว่าโปรแกรมไวรัส (Program Viruses) ไวรัสจำพวกนี้จะเกาะติดกับไฟล์นามสกุล .exe หรือ .com หรือ .sys เมื่อโปรแกรมที่ติดไวรัสถูกเรียกขึ้นมา ไวรัสก็จะทำงานโดยมาฝังตัวในหน่วยความจำก่อน แล้วให้โปรแกรมทำงานตามปกติต่อไป หลังจากนั้นถ้ามีการเรียกโปรแกรมอื่นๆ ขึ้นมาทำงานต่อ ตัวไวรัสก็จะ

สำเนาตัวเองเข้าไปในโปรแกรมเหล่านั้นทันที จงจำไว้ว่าไวรัสคอมพิวเตอร์นั้นทำงาน*เงียบๆ* ไม่มีหน้าต่างขึ้นมาติดต่อกับผู้ใช้

๑.๑.๓ มาโครไวรัส (Macro Viruses) เป็นไวรัสที่ใช้ความสามารถของชุดโปรแกรมไมโครซอฟท์ออฟฟิศ (Microsoft Office) ในการเขียนโค้ดภาษามาโคร (Macro Language) โดยไวรัสจำพวกนี้จะเน้นก่อกวนในไฟล์เอกสาร ซึ่งจะทำให้เครื่องช้าหรือค้าง เป็นต้น

ถ้าจะกล่าวโดยสรุปสำหรับไวรัสก็คือ ไวรัสนั้นสร้างความเสียหายให้กับไฟล์ สำหรับสิ่งที่เกี่ยวกับไวรัสเพิ่มเติมก็คือ ไวรัสตัวแรก พบเมื่อ พ.ศ. ๒๕๑๓ (ค.ศ. ๑๙๗๐) ชื่อ Creeper บน ARPANET อาการของไวรัสตัวนี้ก็คือ จะมีข้อความว่า “I’m the creeper,Catch me if you can!” ปรากฏขึ้นมา หลังจากนั้นไม่นานก็มีตัวกำจัดชื่อ Reeper มาแก้ไข ส่วนไวรัสตัวแรกของไทยพบเมื่อ พ.ศ. ๒๕๓๔ (ค.ศ.๑๙๙๑) ชื่อ ลาวดวงเดือน

๑.๒ เวิร์ม (Worm)

บางทีเราเรียกว่า หนอน หรืออาจจะเรียก พยาธิ ก็แล้วแต่ เวิร์มเป็นมัลแวร์อีกตัวหนึ่ง ซึ่งสามารถแพร่กระจายจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งโดยอาศัย อีเมล หรือช่องโหว่ของระบบปฏิบัติการ Windows (เช่น พอร์ต ๑๓๗-๑๓๙,๔๔๕ หรือพอร์ตอื่นๆ อีกมากมาย) ซึ่งเป็นการแชร์ในระบบเครือข่าย สิ่งที่เวิร์มทำมักจะสร้างความเสียหายให้กับข้อมูลและแบนด์วิธในระบบเครือข่าย เช่น การแพร่กระจายเชื้อซ้ำๆ กัน เป็นจำนวนมาก จนทำให้ระบบเครือข่ายล่ม

กล่าวโดยสรุปของเวิร์มก็คือ สร้างความเสียหายให้กับระบบเครือข่ายและการใช้งานอินเทอร์เน็ต

๑.๓ สปายแวร์ (Spyware)

เป็นมัลแวร์ที่ไม่ได้มีจุดประสงค์เพื่อทำลาย แต่รบกวนและสร้างความรำคาญให้กับผู้ใช้ โปรแกรมพวกนี้จะคอยจับความเคลื่อนไหว ตลอดจนการใช้งานของเรา แล้วรวบรวมข้อมูลดังกล่าวส่งไปยังผู้สร้างมัน นอกจากนี้ยังเปลี่ยนการตั้งค่าของบราวเซอร์ (Browser) ซึ่งอาจจะเป็นโฆษณาสินค้าแทนก็ได้

๑.๔ แอดแวร์ (Adware)

เป็นโปรแกรมลักษณะคล้ายสปายแวร์ เพื่อหวังผลโฆษณาสินค้า แต่แอดแวร์จะติดในเครื่องคอมพิวเตอร์ได้ก็เพราะเกิดจากการหลอกล่อให้โหลดไฟล์ต่างๆ มา หรือการให้สิทธิในการใช้โปรแกรมฟรีแลกกับการมีพื้นที่โฆษณาในโปรแกรมนั้นๆ แต่แอดแวร์นั้นไม่สามารถแพร่เชื้อไปยังเครื่องอื่นได้

๑.๕ โทรจัน (Trojan)

ถูกออกแบบมาให้แฝงตัวหรืออำพรางตัวมันเองเข้ามาในระบบคอมพิวเตอร์ และทำงานโดยการดักจับข้อมูล เช่น รหัสผ่านในการเข้าใช้งานระบบต่างๆ แล้วส่งข้อมูลไปยังผู้ที่สร้างมันขึ้นมา เพื่อเข้าใช้หรือโจมตีระบบ หรือเข้ามาควบคุมเครื่องเราเพื่อไปโจมตีเครื่องอื่นๆ ในระบบเครือข่ายอินเทอร์เน็ต การจะติดโทรจันนั้น โทรจันจะอาศัยการหลอกล่อให้เราโหลดโปรแกรมมาหรือติดกับดักที่ถูกส่งมาทางอีเมลที่ถูกบรรจุมากับข้อความที่ดูเหมือนธรรมดา แต่เมื่อมีการเปิดอ่านมันก็จะอาศัยตัวกลางที่อาจจะเป็นโปรแกรมที่แนบมาพร้อมกับอีเมล สั่งให้โทรจันทำงานและเปิดช่องทางต่างๆ เพื่อจะเข้ามาควบคุมหรือโจมตีระบบคอมพิวเตอร์

๑.๖ โพลีมอร์ฟิกมัลแวร์ (Polymorphic Malware)

เป็นมัลแวร์ที่มีความสามารถในการเปลี่ยนแปลงตัวเองได้หลายรูปแบบ ซึ่งจะทำให้ยากต่อการที่โปรแกรมป้องกันไวรัสคอมพิวเตอร์จะตรวจสอบได้

๑.๗ สทีลต์มัลแวร์ (Stealth Malware)

เป็นมัลแวร์ที่มีความสามารถในการพรางตัวต่อการตรวจจับของโปรแกรมป้องกันไวรัสคอมพิวเตอร์ เช่น การเข้าไปควบคุมการทำงานของโหมดดอส (Command Prompt) กรณีใช้คำสั่ง DIR เพื่อดูขนาดของไฟล์หรือโปรแกรม ก็จะแสดงขนาดเหมือนเดิม เหมือนไม่มีอะไรเกิดขึ้น

ดังนั้นในที่นี้เพื่อความเข้าใจร่วมกันจะขอเรียกมัลแวร์ทั้งหมดรวมๆ กันว่า ไวรัสคอมพิวเตอร์ก็แล้วกัน เพราะว่าโปรแกรมที่ใช้ป้องกันหรือกำจัดมัลแวร์ ก็ไม่ได้มีการเรียกว่า โปรแกรมป้องกันมัลแวร์ หรือ AntiMalware แต่จะเรียกว่า โปรแกรมป้องกันไวรัส หรือ AntiVirus แทน ซึ่งหากจะมีการกล่าวเพื่อชี้ชัดมัลแวร์บางตัว ก็จะกล่าวเฉพาะเจาะจงลงไป ดังนั้นเพื่อความเข้าใจในส่วนนี้ด้วย ว่าถ้ากล่าวถึงไวรัสคอมพิวเตอร์ตั้งแต่นี้ไปในหนังสือเล่มนี้ ก็คือมัลแวร์นั่นเอง

๒. ลักษณะอาการของเครื่องที่ติดไวรัสคอมพิวเตอร์

ถ้าจะป้องกันและกำจัดไวรัสคอมพิวเตอร์ ผู้เขียนเชื่อว่าทุกคนถ้าใช้คอมพิวเตอร์ของตัวเองที่ใช้งานเป็นประจำ จะมีความรู้สึกหรือรับรู้ได้ ถ้าคอมพิวเตอร์ที่เราใช้งานเป็นประจำนั้นมีอาการผิดปกติ ดังนั้นสิ่งหนึ่งที่เราต้องรู้ คือการสังเกตการทำงานของคอมพิวเตอร์ด้วยว่ามีอาการดังต่อไปนี้

๑. ไม่สามารถดับเบิลคลิกเปิดโปรแกรม ไดรฟ์ แฟลชไดรฟ์ ได้ หรือใช้เวลา นาน ผิดปกติในการเรียกโปรแกรมขึ้นมาทำงาน
๒. คลิกเมาส์ขวาไม่ได้
๓. วัน เวลาของโปรแกรมเปลี่ยนไป
๔. ไม่สามารถใช้งาน Task Manager ได้
๕. คอมพิวเตอร์ทำงานช้าลง
๖. ไฟล์และโฟลเดอร์หายไป
๗. แป้นพิมพ์ทำงานผิดปกติ หรือไม่ทำงานเลย
๘. คอมพิวเตอร์รีสตาร์ทตัวเอง หรือ บูตตัวเองขึ้นมาโดยไม่ได้สั่ง
๙. มีเมนูหรือข้อความที่ปกติไม่เคยเห็นถูกแสดงขึ้นมา
๑๐. ขนาดไฟล์ใหญ่ขึ้นผิดปกติ โดยเฉพาะไฟล์ .exe

สิ่งต่างๆ ที่กล่าวมานี้ คือ อาการผิดปกติ โดยทั่วๆ ไป ที่ผู้ใช้รับรู้ได้ แต่มิได้หมายความหรือเป็นข้อสรุปว่าอาการดังกล่าวติดไวรัสคอมพิวเตอร์เสมอไป บางทีก็อาจจะเกิดจากอุปกรณ์ฮาร์ดแวร์ของคอมพิวเตอร์เองก็เป็นได้ ทั้งนี้ผู้เขียนเชื่อว่าผู้ใช้ทุกคนสามารถจำแนกหรือรู้ว่าเกิดอะไร เพราะเป็นเครื่องที่ตัวเองใช้เป็นประจำ

๓. กฎพื้นฐานในการป้องกันไวรัสคอมพิวเตอร์

สำหรับผู้ที่ไม่ต้องการเรียนรู้วิธีการป้องกันหรือเทคนิคในการจัดการไวรัสคอมพิวเตอร์ด้วยตนเองนั้น มีแนวทางในการป้องกันไวรัสคอมพิวเตอร์เบื้องต้น ดังนี้

๑. ลบไฟล์ขยะทิ้ง *(แต่ส่วนมากผู้ใช้จะไม่เคยทำเลย)*

๒. สแกนสื่อทุกชนิดก่อนใช้งาน *(แต่ผู้ใช้ส่วนมากจะลืมหรือไม่ก็เพราะเผลอ)*
๓. หลีกเลี่ยงการเข้าเว็บที่เสี่ยงอันตราย *(แต่ผู้ใช้ก็จะมีนิสัยไม่ลองไม่รู้ หรืออาจจะถูกหลอกให้เข้าไปใช้เว็บที่เสี่ยงนั้นๆ)*
๔. หลีกเลี่ยงการเปิดไฟล์จากเมล์ที่ไม่รู้จัก *(แต่ผู้ใช้โดยส่วนมากก็จะอยากรู้อยากเห็น กลัวตกข่าวสำคัญ หารู้ไม่ว่านั่นคือสิ่งที่ทำให้ติดไวรัสคอมพิวเตอร์)*
๕. อัพเดทโปรแกรมป้องกันไวรัสให้ทันสมัย *(แต่ผู้ใช้ส่วนมากทำไม่ได้เพราะโปรแกรมป้องกันไวรัสที่ติดตั้งในเครื่องคอมพิวเตอร์ ไม่ใช่โปรแกรมลิขสิทธิ์)*

แต่สำหรับผู้ที่ต้องการเรียนรู้เทคนิคในการต่อกรกับไวรัสคอมพิวเตอร์ด้วยตนเองนั้น เราจะได้มาเรียนรู้กันในหนังสือเล่มนี้ ซึ่งแนวทางเบื้องต้นก็คือ ปรับเปลี่ยนลักษณะวิธีใช้ และการตรวจสอบด้วยตัวเราเองตามวิธีการและแนวทางที่จะจัดการกับไวรัสคอมพิวเตอร์ที่จะกล่าวถึงในบทต่อไป

๔. โปรแกรมป้องกันไวรัสคอมพิวเตอร์แบบฟรีแวร์

มีโปรแกรมป้องกันไวรัสคอมพิวเตอร์หลายตัวที่เป็นฟรีแวร์ เราสามารถดาวน์โหลดมาใช้ได้โดยไม่ต้องเสียค่าลิขสิทธิ์ แต่เราก็อาจจะไม่ได้ประสิทธิภาพที่สูงสุดก็ได้ ซึ่งเราสามารถหาได้โดยใช้ Search Engine อย่าง Google ในการค้นหาซึ่งมีมากมายหลายชนิด ผู้เขียนไม่ขอกล่าวถึง เพราะในหนังสือเล่มนี้ก็มิได้ใช้โปรแกรมจำพวก AntiVirus อยู่แล้ว

๕. เรียนรู้และเข้าใจหลักการตรวจหาไวรัสคอมพิวเตอร์ของโปรแกรมป้องกันไวรัสคอมพิวเตอร์

โปรแกรมป้องกันไวรัสคอมพิวเตอร์จะมีรูปแบบในการตรวจหาไวรัสคอมพิวเตอร์ ซึ่งพอจะจำแนกได้ดังต่อไปนี้ คือ

๕.๑ วิธีการสแกนเนอร์

การสแกนเนอร์เป็นวิธีหนึ่งในการตรวจสอบไวรัสคอมพิวเตอร์โดยจะดึงเอาโปรแกรมบางส่วนของตัวไวรัสคอมพิวเตอร์มา ซึ่งเรียกว่า ไวรัสซิกเนเจอร์ (Virus Signature) โดยการนำมาเก็บไว้เป็นฐานข้อมูล เมื่อตัวตรวจสอบไวรัสคอมพิวเตอร์แบบสแกนเนอร์ถูกเรียกขึ้นมาทำงาน ก็จะตรวจหาไวรัสคอมพิวเตอร์ในหน่วยความจำ บูตเซคเตอร์ และไฟล์ โดยใช้ฐานข้อมูลไวรัสซิกเนเจอร์ที่มีอยู่ ซึ่งข้อดีของวิธีการแบบนี้ คือ สามารถตรวจสอบไวรัสคอมพิวเตอร์ ที่มากับซอฟท์แวร์ใหม่ได้ทันที เพื่อป้องกันไม่ให้ไวรัสคอมพิวเตอร์ถูกเรียกขึ้นมาทำงานตั้งแต่เริ่มต้น แต่ก็มีข้อเสียคือ

๑. ฐานข้อมูลที่เก็บไวรัสซิกเนเจอร์ต้องทันสมัยและครอบคลุมไวรัสคอมพิวเตอร์ทุกตัว เพราะสแกนเนอร์จะไม่สามารถตรวจสอบไวรัสคอมพิวเตอร์ที่ยังไม่มีอยู่ในฐานข้อมูล ดังนั้นผู้ใช้ต้องหาสแกนเนอร์ตัวที่ใหม่ที่สุดมาใช้เสมอ
๒. ถ้าเครื่องมีไวรัสคอมพิวเตอร์อยู่แล้ว และสแกนเนอร์ไม่สามารถตรวจจับได้ ในขณะที่สแกนเนอร์จะเข้าไปอ่านโปรแกรมทีละโปรแกรมเพื่อตรวจสอบ ผลก็คือจะทำให้ไวรัสคอมพิวเตอร์ที่มีอยู่ไปติดในโปรแกรมทุกตัวที่สแกนเนอร์นั้นอ่าน

๕.๒ วิธีการตรวจการเปลี่ยนแปลง

คือ การหาค่าพิเศษอย่างหนึ่งที่เรียกว่า เช็คซัม (Checksum) ซึ่งเกิดจากการนำเอาชุดคำสั่งและข้อมูลที่อยู่ในโปรแกรมมาคำนวณ หรืออาจจะใช้ข้อมูลของไฟล์ เช่น วัน เวลา แอดตริบิวต์ (Attribute) เข้ามาใช้ในการคำนวณด้วย ซึ่งวิธีการคำนวณหาค่าเช็คซัมมีหลายแบบที่แตกต่างกันออกไป เมื่อตัวโปรแกรมภายในเกิดการเปลี่ยนแปลง ไม่ว่าไวรัสคอมพิวเตอร์จะใช้วิธีการแทรกหรือเขียนทับ เลขที่ได้จากการคำนวณครั้งใหม่จะเปลี่ยนแปลงไปจากที่ได้จากการคำนวณก่อนหน้านี้

ข้อดีของวิธีการนี้ ก็คือ สามารถตรวจจับไวรัสคอมพิวเตอร์ใหม่ๆ ได้ แต่วิธีการดังกล่าวนี้จะตรวจจับไวรัสคอมพิวเตอร์ได้ เมื่อไวรัสคอมพิวเตอร์ได้เข้าไปติดอยู่ในคอมพิวเตอร์ แล้ว ดังนั้นวิธีการนี้ต้องแน่ใจว่าเครื่องคอมพิวเตอร์เราปลอดภัยพอ เพราะถ้ามีการเริ่มคำนวณในเครื่องที่ติดไวรัสคอมพิวเตอร์อยู่ก่อนที่จะนำโปรแกรมป้องกันไวรัสประเภทนี้ไปใส่ ก็จะไม่มีประโยชน์ใดๆ เลย

๕.๓ วิธีการเฝ้าดู

โดยเทคนิคก็คือใช้วิธีการสแกนเนอร์ หรือการตรวจการเปลี่ยนแปลง หรือทั้งสองอย่างรวมกันก็ได้ การทำงานก็คือ เมื่อโปรแกรมตรวจจับไวรัสคอมพิวเตอร์ที่ใช้วิธีการเฝ้าดูนี้ถูกเรียกขึ้นมา ก็จะเข้าไปตรวจในหน่วยความจำของเครื่องคอมพิวเตอร์ก่อนว่ามีไวรัสคอมพิวเตอร์ติดอยู่หรือไม่ โดยใช้ไวรัสซิกเนเจอร์ จากนั้นก็นำตัวเองไปอยู่ในหน่วยความจำ และต่อไปถ้ามีการเรียกโปรแกรมใดขึ้นมาใช้งาน โปรแกรมเฝ้าดูนี้ก็จะเข้าไปตรวจโปรแกรมนั้นก่อน โดยใช้เทคนิคการสแกนเนอร์หรือตรวจการเปลี่ยนแปลงเพื่อหาไวรัสคอมพิวเตอร์ ถ้าไม่มีปัญหาก็จะอนุญาตให้โปรแกรมนั้นทำงาน แต่ปัญหาของโปรแกรมเฝ้าดูนี้ก็คือ จะใช้หน่วยความจำของเครื่องคอมพิวเตอร์ส่วนหนึ่งตลอดเวลา ถ้าเครื่องคอมพิวเตอร์มีหน่วยความจำน้อย ก็จะทำให้เครื่องคอมพิวเตอร์ทำงานช้าลงไปอย่างมาก

๖. สรุป

จากที่ได้กล่าวมาทั้งหมดจะเห็นว่าถ้าอาศัยโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ก็ไม่ได้มีเครื่องหมายการันตีว่าเครื่องคอมพิวเตอร์จะปลอดภัยจากไวรัสคอมพิวเตอร์เสมอไป และถ้าต้องเสาะหาโปรแกรมป้องกันไวรัสใหม่ๆ มาใส่อยู่เสมอ เราคงหาเงินเพื่อมาเป็นค่าซื้อโปรแกรมดังกล่าวกันไม่สิ้นสุด

ดังนั้นวิธีการต่อไปในหนังสือเล่มนี้ก็คือจะพาทุกท่านใช้หนึ่งสมองและสองมือของเราใช้เทคนิคง่ายๆ ในการจัดการไวรัสคอมพิวเตอร์ด้วยตนเอง อาจจะมีบ้างที่ใช้ซอฟท์แวร์ช่วย แต่ก็เป็นซอฟท์แวร์ประเภทฟรีแวร์ที่ไม่ต้องเสียเงินซื้อหา และไม่ละเมิดลิขสิทธิ์ใครอีกด้วย

และในหนังสือเล่มนี้เช่นเดียวกันคำว่า ระบบปฏิบัติการวินโดวส์ หมายถึง ระบบปฏิบัติการวินโดวส์ ๗ (Widows ๗) และหรือระบบปฏิบัติการวินโดวส์ ๘ (Windows ๘) เพราะระบบปฏิบัติการวินโดวส์ก่อนหน้านี้คงหาผู้ใช้ได้น้อยแล้ว