MALWARE

มัลแวร์

หลักสูตรปฏิบัติการสงครามไซเบอร์

ร.ท.ธนาสิน นารีแก้ว

นายทหารปฏิบัติการ แผนกตอบสนองภัยคุกคามทาง กรซ.ศซบ.สสท.ทร.

หัวข้อการบรรยาย

- วิวัฒนากาของมัลแวร์
- มัลแวร์ประเภทต่าง ๆ
- คุณสมบัติและวงจรชีวิตของมัลแวร์
- มัลแวร์ที่มีชื่อเสียง
- ซอฟต์แวร์ป้องกันมัลแวร์
- การป้องกันมัลแวร์

วิวัฒนาการของมัลแวร์

ไวรัสคอมพิวเตอร์ที่พบในช่วงแรก เป็นไวรัสที่พัฒนาเพื่อใช้ในห้องทดลองเท่านั้น ซึ่งลักษณะของไวรัสนั้นก็เป็นไฟล์ที่สามารถก็อปปี้ตัวเองไปเรื่อย ๆ และเมื่อถูกรันก็แค่แสดงข้อความตลก ๆ หรือคำไม่สุภาพเท่านั้น การที่จะบอกว่าไวรัสนั้นเริ่มมีเมื่อไรหรือมาจากไหนนั้นเป็นสิ่งที่ยาก เนื่องจากโดยธรรมชาติแล้วผู้ที่สร้างไวรัสนั้นส่วนใหญ่จะไม่ค่อยเปิดเผยตัวเองนอกจากจะถูกบหาจนเจอ

วิวัฒนาการของมัลแวร์

ปี ค.ศ. 1969 ทีมวิศวกรห้องทดลองระบบโทรศัพท์ของบริษัท เบลล์ ได้สร้างเกมชื่อว่า ดาร์วิน (Darwin) ซึ่งถือว่าเป็นโปรแกรมคอมพิวเตอร์แรกที่มีรูปแบบคล้ายไวรัส โดยโปรแกรมจะฝังตัวอยู่ในหน่วยความจำ เกมนี้ใช้คำศัพท์บางอย่างที่มีคำว่า "supervisor“ มีลักษณะที่กำหนดกฎเกณฑ์การต่อสู้ระหว่างผู้เข้าแข่งขัน โปรแกรมดาร์วินนี้มีความสามารถที่จะวิจัยสภาพแวดล้อมของมัน ทำสำเนาตัวเอง และทำลายตัวเองได้ จุดประสงค์หลักของเกมนี้ก็คือ ลบโปรแกรมทั้งหมดที่คู่แข่งเขียนแล้วครอบครองสนามรบ

วิวัฒนาการของมัลแวร์

ปี ค.ศ. 1970 มีการตรวจพบไวรัสครีเปอร์ (Creeper) ในเครือข่าย APRA net ซึ่งเป็นเครือข่ายที่ใช้ในด้านการทหารในประเทศสหรัฐอเมริกัน ไวรัสนี้ถือเป็นต้นแบบของไวรัสคอมพิวเตอร์ในปัจจุบัน เพราะโปรแกรมครีเปอร์สามารถแพร่กระจายตัวเองผ่านเครือข่ายโมเด็ม โดยการส่งสำเนาตัวเองไปยังเครื่องอื่น เมื่อติดไวรัสนี้แล้วก็จะแสดงข้อความว่า "I'M THE CREEPER ... CATCH ME IF YOU CAN" (ฉันเป็นคนสร้างสรรค์...จับฉันสิถ้าคุณทำได้)

วิวัฒนาการของมัลแวร์

ปี ค ศ. 1974 โปรแกรมชื่อ "Rabbit" โผล่ขึ้นมาบนเครื่องเมนเฟรม ที่เรียกชื่อนี้เพราะมันไม่ได้ทำอะไรนอกจากสำเนาตัวเองอย่างรวดเร็วไปในระบบเก็บข้อมูลชนิดต่าง ๆ Rabbit นี้ได้ดึงทรัพยากรของระบบมาใช้อย่างมาก ทำให้กระทบต่อการทำงานอย่างรุนแรงจนอาจทำให้ระบบทำงานผิดพลาดได้

วิวัฒนาการของมัลแวร์

ปี ค.ศ. 1982 มีการตรวจพบไวรัสชื่อ “elk Cloner" ซึ่งเป็นคอมพิวเตอร์ไวรัสบนเครื่องพีซีตัวแรก ซึ่งแพร่กระจายในวงที่กว้างออกไปกว่าภายในห้องทดลองที่สร้างโปรแกรม โดยไวรัสนี้จะติดไปกับระบบปฏิบัติการ Apple Dos 3.3 ผ่านทางบู๊ตเซ็กเตอร์ของฟล็อปปี้ดิสก์ ณ เวลานั้น ผลของมันทำให้ผู้ใช้คอมพิวเตอร์บางคนนึกว่าไวรัสคอมพิวเตอร์เกิดจากมนุษย์ต่างดาว เพราะทำให้การแสดงภาพที่จอกลับหัว ทำตัวอักษรกะพริบขึ้นข้อความต่าง ๆ ออกมา

วิวัฒนาการของมัลแวร์

ปี ค.ศ. 1983 Len Adleman แห่งมหาวิทยาลัย Lehigh ตั้งคำว่า "Virus“ ว่าเป็นโปรแกรมคอมพิวเตอร์ที่ทำสำเนาตัวเองได้ และในปีถัดมาในการประชุมสัมมนาด้านการรักษาความปลอดภัยข้อมูล ครั้งที่ 7 เฟรด โคเฮน (Fred Cohen) ได้ให้คำจำกัดความของคำว่า "Computer Virus" ว่าเป็นโปรแกรมที่สามารถติดต่อไปยังโปรแกรมอื่น โดยการแก้ไขโปรแกรมเดิมเพื่อแพร่กระจายตัวเอง ซึ่งเขาได้ใช้คอมพิวเตอร์ VAX 11/750 สาธิตว่าโปรแกรมไวรัสสมารถฝังตัวเข้าไปในออบเจ็กต์อื่นได้ ซึ่งต่อมาเขาได้รับการยกย่องให้เป็นบิดาแห่งไวรัสศาสตร์ (Virology)

วิวัฒนาการของมัลแวร์

ปี ค.ศ. 1988 ปีเตอร์ นอร์ตัน (Peter Norton) โปรแกรมเมอร์ที่มีชื่อเสียงผู้ซึ่งเป็นผู้ก่อตั้งบริษัท ไซแมนเทค (Symantec) ได้ออกมาประกาศว่าไวรัสคอมพิวเตอร์เป็นเรื่องไร้สาระ โดยเปรียบว่าเป็นแค่จระเข้ที่อยู่ในท่อระบายน้ำเสียในนิวยอร์ก แต่ในที่สุดเขาเป็นผู้ที่ได้เริ่มต้นพัฒนาโปรแกรมป้องกันมัลแวร์ Norton - Anti Virus ซึ่งออกมาวางขายในปี ค.ศ. 1991

วิวัฒนาการของมัลแวร์

ปี ค.ศ. 1988 เดือนตุลาคม มีการแพร่ข่าวไวรัสชื่อ "Mr.RoChenle“ ซึ่งเป็นไวรัสประเภทหลอกลวงหรือโฮคซ (HOAX) เป็นตัวแรกโปรแกรมนี้จะแสดงผลโดยการอ้างถึงชื่อบุคคลที่ไม่มีตัวตนชื่อ Mike RoChenle ("Microchannel") และอ้างว่าไวรัสนี้สมารถแพร่กระจายตัวเองไปบนโมเต็มด้วยความเร็ว 2,400 bps นอกจากนี้ยังทำให้ความเร็วโมเค็มลดลงเหลือ 1,200 bps และได้อธิบายวิธีการแก้ไขที่ไม่ได้มีผลอะไร แต่มีคนหลงเชื่อทำตามกันอย่างมากมาย

วิวัฒนาการของมัลแวร์

ปี ค.ศ. 1999 ไวรัสที่ชื่อ "Melissa“ ถูกเขียนโดย เดวิด แอล สมิธ เป็นไวรัสที่แพร่กระจายผ่านอีเมลโดยการอ่านรายชื่อที่อยู่อีเมลจากไมโครซอฟท์เอาต์ลุค โดยมีการติดจำนวนมากจนทำให้ระบบอีเมลอินเทอร์เน็ตแทบใช้งานไม่ได้ และสร้างความเสียหายประมาณ 80 ล้านดอลลาร์

วิวัฒนาการของมัลแวร์

ปี ค.ศ. 2000 ไวรัสที่ชื่อ "I Love You" ถูกเขียนโดยนักเรียนชาวฟิลิปปินส์ ซึ่งไวรัสตัวนี้ก็คล้ายกับ Melissa ที่อาศัยอีเมลในการแพร่กระจายตัวเอง ต่อมาในปี ค.ศ. 2001 เวิร์มโค้ดเร้ด (Code Red) เวิร์มได้ติดมากกว่าล้านเครื่องที่ใช้ระบบปฏิบัติการวินโดวส์ NT2000 เซิร์ฟเวอร์ ต่อมาในปีเดียวกันเวิร์มนิมด้า(Nim da)ใช้เทคนิคคล้าย ๆ กันในการแพร่กระจายผ่านเครือข่าย แต่สามารถแพร่กระจายได้มากที่สุดภายในเวลา 22 นาที โดยได้โจมตีระบบไมโครซอฟท์วินโดวส์ ชื่อนิมด้า (Nim da) นั้นมาจากการอ่านคำว่า แอดมิน (Admin) กลับหลังนั้นเอง ในปี 2003 เวิร์มที่ชื่อ "Slammer" เป็นเวิร์มที่มีการแพร่กระจายได้เร็วที่สุดและติดเครื่องหลายแสนเครื่องที่ติดตั้งไมโครซอฟท์ SQL เซิร์ฟเวอร์ และในปีเดียวกันนี้ก็มีเวิร์มชื่อ "Blaster" หรือ "Love san" ซึ่งเป็นเวิร์มที่ใช้ประโยชน์จากช่องโหว่ของระบบวินโดวส์

วิวัฒนาการของมัลแวร์

ปี ค.ศ. 2004 เวิร์มมายดูม (My Doom) ได้แพร่กระจายตัวเองได้เร็วที่สุดเท่าที่เคยมีมา โดยแพร่กระจายตัวเองผ่านระบบอีเมลเหมือน Melissa และ I Love You และในปีเดียวกันเวิร์ม "Sasser" ก็ได้แพร่กระจายโดยใช้ช่องโหว่ของระบบ LSASS (Local Security Authority Subsystem Service) ของวินโดวส์

วิวัฒนาการของมัลแวร์

ปี ค.ศ. 2007 เวิร์มซีส (Zeus) ได้แพร่ระบาดโดยเป็นเครื่องมือสำหรับสร้างบอตเน็ต เพื่อขโมยและรวบรวมข้อมูลโดยเฉพาะข้อมูลที่ใช้ระบุตัวตนและรหัสผ่านสำหรับระบบอินเทอร์เน็ตแบ๊งกิ้ง แต่ยังสามารถขโมยข้อมูลอื่น ๆ จากเครื่องของผู้ใช้งานได้อีกด้วย

วิวัฒนาการของมัลแวร์

ปี ค.ศ. 2009 เวิร์มคอนฟิกเกอร์ (Conficker) หรืออีกชื่อหนึ่คือ ดาวน์อัพ (Downup) ได้โจมตีระบบไมโครซอฟท์วินโดวส์กว่า 15 ล้านครื่องทั่วโลก โดยที่ไม่มีการช่วยเหลือจากผู้ใช้เลย คอนฟิกเกอร์ใช้ประโยชน์จากช่องโหว่ของระบบซึ่งยากต่อการตรวจจับโดยโปรแกรมป้องกันมัลแวร์ นอกจากจะอัพเดตซิกเนเจอร์ให้ทันสมัย คอนฟิกเกอร์จะสร้างชอมบี้ ซึ่งเป็นสมุนของบอตเน็ต กี่จะใช้ในการขโมยข้อมูลจากเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ไม่รู้ตัว

วิวัฒนาการของมัลแวร์

ปี คศ. 2013 คริพโตล็อกเกอร์ (Cryptolocker) เป็นโทรจันฮอร์สเรียกค่าไถ่ที่โจมตีระบบคอมพิวเตอร์ที่รันไโครซอฟท์วินโคว เมื่อโจมตีแล้วมัลแวร์จะเข้ารหัสไฟล์บางไฟล์ในระบบโดยใช้การเข้ารหัสแบบ RSA พับลิกคีย์ โดยไพรเวทดีย์นั้นจะเก็บไว้ที่เซิฟวอร์ควบคุมของมัลแวร์ที่เดียว แล้วมัลแวร์ก็จะทำการเรียกค่าไถ่ โดยให้จ่ายเงินผ่าน Bitcoin หรือบัตรเครดิตในวลาที่กำหนด หากไม่จ่ายเงิน คริพโตล็อกเกอร์ก็จะลบไฟล์ทิ้ง แต่ถ้าจ่ายเงินผู้ใช้ก็จะได้ไพรเวทดีย์ที่จะใช้สำหรับการถอดรหัสไฟล์นั้น ๆ

คุณลักษณะของมัลแวร์ในปัจจุบัน

ความเร็วในการโจมตี

ด้วยความสามารถของเครื่องมือสมัยใหม่และความง่ายในการได้มา ซึ่งเครื่องมือเหล่านี้ทำให้ผู้โจมตีสมารถสแกน เพื่อค้นหาเป้าหมายที่มีจุดอ่อนหรือช่องโหว่ และโจมตีด้วยความรวดเร็ว (Speed of Attacks) ยกตัวอย่างเช่น ในปี 2003 สแลมเมอร์เวิร์ม (Slammer Worm) สามารถทำลายกว่า 75,000 คอมพิวเตอร์ภายในเวลาเพียง 11 นาทีแรก นับจากจุดเริ่มต้นของการโจมตี และสามารถแพร่กระจายได้เป็นเท่าตัวทุก ๆ 85 วินาที และที่จุดสูงสุดสแลมมอร์เวิร์มสามารถสแกน 55 ล้านเครื่องต่อวินาทีเพื่อค้นหาคอมพิวเตอร์ที่จะทำลาย และต่อมาในปีเดียวกันบลาสเตอร์เวิร์ม (Blaster Worm) สามารถแพร่กระจายตัวเองไปยังกว่า 138,000 เครื่องในช่วง 4 ชั่วโมงแรกของการโจมตี และสามารถติดเชื้อกว่า 1.4 ล้านเครื่อง เครื่องมือสำหรับการโจมตีในปัจจุบันนั้น สามารถโจมตีเองได้โดยไม่ต้องอาศัยมนุษย์ จึงทำให้ความเร็วในการโจมตีนั้นเพิ่มขึ้นเรื่อย ๆ

คุณลักษณะของมัลแวร์ในปัจจุบัน

ความซับซ้อนในการโจมตี

การโจมตีในปัจจุบันมีความซับซ้อนเพิ่มมากขึ้นเรื่อย ๆ บางเครื่องมือที่ใช้สำหรับการโจมตีมีความหลากหลายในตัวเอง ทำให้สามารถโจมตีเดียวกันแต่มีความแตกต่างในแต่ละครั้งที่โจมตี ทำให้การตรวจจับนั้นทำได้ยาก การโจมตีนั้นได้หันมาใช้โปรโตคอลที่ใช้เป็นประจำอย่างเช่น HTTP (Hypertext Transfer Protocol) เพื่อสำหรับส่งข้อมูลและคำสั่งเพื่อโจมตีคอมพิวเตอร์ ทำให้ยากที่จะแยกความแตกต่างระหว่างการโจมตีและการใช้งานปกติ

คุณลักษณะของมัลแวร์ในปัจจุบัน

ความรวดเร็วในการค้นหาจุดอ่อน

จำนวนของช่องโหว่หรือจุดอ่อน (Vulnerability) ใหม่ที่ค้นพบในแต่ละปีนั้นเพิ่มขึ้นเป็นสองเท่าทุกปี จนบางครั้งทำให้ผู้พัฒนาซอฟต์แวร์อัพเดตหรือปิดช่องโหว่ไม่ทัน และสิ่งที่น่ากลัวที่สุดคือ การโจมตีแบบ Zero-day attack ซึ่งหมายถึง การโจมตีที่เกิดขึ้นโดยผู้โจมตีนั้นสามารถค้นหาช่องโหว่เอง โดยที่ช่องโหว่นี้ยังไม่มีใครค้นพบมาก่อน และสร้างเครื่องมือในการโจมตีผ่านช่องโหว่นี้ทำให้เป้าหมายนั้นไม่มีทางรู้เลยว่าถูกโจมตีผ่นช่องโหว่ใดและยิ่งเป็นการยากและใช้เวลานานมากขึ้นในการแก้ปัญหาการโจมตีประเภทนี้

คุณลักษณะของมัลแวร์ในปัจจุบัน

การโจมตีแบบแยกกระจาย

ปัจจุบันผู้โจมตีสามารถใช้คอมพิวเตอร์หลายพันหลายแสนเครื่องเพื่อโจมตีเป้าหมายเดียวกัน (Distributed attack) โดยขั้นตอนแรกนั้นนักโจมตีก็จะค้นหาเครื่องร่วมโจมตี ฝังโด้ดและตั้งเวลาในการโจมตีพร้อมกัน การโจมตีแบบแยกกระจายนี้ทำให้ยากต่อการป้องกันและหยุดยั้งการโจมตีได้เพราะแหล่งที่มานั้นมากเกินไปที่จะสามารถบล็อคได้

คุณลักษณะของมัลแวร์ในปัจจุบัน

ความขับซ้อนในการติดตั้งแพตช์

การป้องกันการโจมตีในรูปแบบต่าง ๆ ที่ได้ผลที่สุดก็คือการติดตั้งแพตช์ (Patch) ซึ่งก็คือชอฟต์แวร์ที่ปิดช่องโหวหรือจุดอ่อนที่มีอยู่ในแอพพลิเคชันหรือระบบปฏิบัติการ อย่างไรก็ตามการจัดการเกี่ยวกับแพตช์และความต้องรู้ว่า จะต้องติดตั้งแพตช์ไหนบ้างกลายเป็นสิ่งที่ยากและซับซ้อน การโจมตีที่สำเร็จโดยส่วนใหญ่นั้น เกิดจากการที่ผู้ใช้ไม่ได้ติดตั้งแพตช์ที่ได้ออกมานาน

ประเภทของมัลแวร์

มัลแวร์ (Malware) ซึ่งย่อมาจากคำว่า Malicious Software เช่น ไวรัส เวิร์ม และโทรจันฮอร์ส ซึ่งเป็นโปรแกรมที่เป็นอันตรายต่อระบบคอมพิวเตอร์ ดังนั้น โปรแกรมไวรัสหรือเวิร์มคืออะไรกันแน่ แล้วแตกต่างจากโทรจันฮอร์สอย่างไร และโปรแกรมป้องกันมัลแวร์ทั่วไปสามารถตรวจพบเวิร์มและโทรจัน ฮอร์สด้วยหรือไม่ หรือใช้ได้กับเฉพาะไวรัส คำถามต่าง ๆ เหล่านี้เกิดขึ้นเนื่องจากความสับสนในคำศัพท์ที่เกี่ยวข้องกับม้แวร์ต่าง ๆ เหล่านี้ และบางทีก็อาจทำให้เข้าใจผิดในบางเรื่องก็ได้ นี่องจากปัจจุบันมัลแวร์มีหลากหลายและแตกต่างกันไป ทำให้ยากต่อการให้คำจำกัดความของโปรแกรมร้าย ๆ แต่ละประเภท

ประเภทของมัลแวร์

เวิร์ม (Worm)

คุณสมบัติพิเศษของเวิร์มคือ มันสามารถแพร่กระจายด้วยตัวของมันเองโดยที่ไม่ต้องอาศัยโปรแกมอื่นในการแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่น ๆ ผ่านทางเครือข่าย เวิร์มสามารถทำอันตรายให้กับระบบ เช่น การใช้แบนด์วิธของเครือข่าย หรือใช้รีซอร์สอื่น ๆ ของเครือข่าย หรือสามารถโจมตีแบบปฏิเสธการให้บริการหรือ DoS (Denial of Service) เวิร์มบางประเภทสามารถแพร่กระจายตัวเองโดยที่ไม่ต้องอาศัยการช่วยเหลือจากผู้ใช้เลย หรือบางตัวก็อาจแพร่กระจายเมื่อผู้ใช้รันโปรแกรมบางโปรแกรมนอกจากความสามารถในการแพร่กระจายด้วยตัวเองแล้ว เวิร์มยังอาจสามารถทำลายระบบได้ด้วย

ประเภทของมัลแวร์

โทรจันฮอร์ส (Trojan Horses)

โทรจันฮอร์สไม่จัดว่าเป็นไวรัสคอมพิวเตอร์หรือเวิร์ม เพราะมันไม่สามารถแพร่กระจายด้วยตัวของมันเอง ไวรัสหรือเวิร์มอาจก็อปปี้โทรจันฮอร์สไปยังระบบอื่นด้วยก็ได้ โดยโทรจันฮอร์สอาจจะเป็นเพย์โหลดของเวิร์มและไวรัส ซึ่งกระบวนการนี้เรียกว่า ดรอปปิง (Dropping) สำหรับเพย์หลดนั้นจะหมายถึง ส่วนโปรแกรมที่จะทำอันตรายต่อระบบเมื่อมีการโจมตีของมัลแวร์เหล่านี้ จุดมุ่งหมายของโทรจันฮอร์สก็เพื่อสร้างความรำคาญให้กับผู้ใช้ หรือขัดขวางการทำงานประจำของระบบ ยกตัวอย่างเช่น โทรจันฮอร์สอาจสร้างแบ็คดอร์ เพื่อเปิดทางให้แฮคเกอร์เข้ามาในระบบเพื่อขโมยข้อมูลหรือเปลี่ยนคอนฟิกของระบบใหม่

ประเภทของมัลแวร์

RAT : Remote Access Trojan

โทรจันฮอร์สบางประเภทจะสร้างแบ็คดอร์ให้แฮคเกอร์เข้ามาในระบบ เพื่อขโมยข้อมูลหรือควบคุมระบบจากระยะไกลได้โปรแกรมประเภทนี้บางทีก็เรียกว่า รีโมทแอ็กเซสโทรจัน (Remote Access Trojan : RAT) หรือแบ็คดอร์ (Back-door) โทรจันฮอร์สที่จัดอยู่ในประเภทนี้ เช่น แบ็คออริฟิซ (Back Orifice), ดาฟีน (Cafeene) และซับเซเว่น (SubSeven) เป็นต้น

ประเภทของมัลแวร์

แบ็คดอร์ (Backdoor)

แบ็คดอร์หรีประตูหลัง เป็นช่องทางพิศษที่ใช้เข้าถึงระบบโดยที่ไม่ต้องผ่านระบบพิสูจน์ทราบตัวตน โดยส่วนใหญ่เมื่อมัลแวร์ติดระบบหรือแฮคเกอร์เจาะเข้าระบบได้แล้ว ก็มักจะวางแบ็คดอร์ไว้เพื่อสำหรับการกลับเข้ามาในระบบในภายหลัง ในสมัยแรก ๆ นั้นแบคดอร์ถูกสร้างไว้โดยเจ้าของผลิตภัณฑ์เอง เพื่อเอาไว้สำหรับให้เจ้าหน้าที่เทคนิครีโมทเข้ามาดูระบบ แต่ในภายหลังช่องทาพิศษนี้ถูกค้นพบโดยแฮคเกอร์ และใช้เจาะเข้าระบบเพื่อทำบางอย่างที่ไม่ดี

ประเภทของมัลแวร์

รูทคิตส์ (Rootkits)

รูทคิตส์ เป็นชุดโปรแกรมที่พวกแฮคคอร์นิยมใช้สำหรับเจาะเข้าระบบ เพื่อควบคุมระบบหรือขโมยข้อมูลโปรแกรมประเภทนี้อาจใช้เทคนิคต่าง ๆ เช่น การเฝ้าดูคีย์สโตรค (Key Stroke) หรือสิ่งที่ผู้ใช้พิมพ์บนคีย์บอร์ด แก้ไขล็อกไฟล์ของระบบ ปิดบางแอพพลิคชันของระบบ สร้างแบ็คดอร์เพื่อสำหรับการเจาะเข้าระบบในภายหลัง หรืออาจใช้ระบบนี้เพื่อเป็นฐานในการโจมตีระบบอื่น ๆ ผ่านทางครือข่าย โดยทั่วไปรูทคิตส์จะถูกจัดไว้เป็นชุดเพื่อใช้สำหรับโจมตีระบบปฏิบัติการประเภทใดประเภทหนึ่งโดยเฉพาะ รูทคิตส์แรกนั้นเกิดขึ้นในปี 1990 ในช่วงนั้นระบบปฏิบัติการซันยูนิกซ์และลีนุกซ์เป็นเป้าหมายของการโจมตี ปัจจุบันมีรูกคิตส์หลายประเภทเพื่อใช้กับระบบปฏิบัติการต่าง ๆ ซึ่งรวมถึงไมโครซอฟท์วินโดวส์

ประเภทของมัลแวร์

ไวรัส (Virus)

ไวรัสเป็นโปรแกรมที่สามารถติดต่อจากไฟล์หนึ่ง ไปยังอีกไฟล์หนึ่งภายในระบบเดียวกันหรือจากคอมพิวเตอร์เครื่องหนึ่งไปเครื่องอื่น โดยการแนบตัวเองไปกับโปรแกรมอื่น มันสามารถทำลายฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล เมื่อโฮสต์รันโปรแกรมที่ติดไวรัส ส่วนที่เป็นไวรัสก็จะถูกรันด้วย และทำให้แพร่กระจายไปยังเครื่องอื่นหรือบางทีก็สร้างโค้ดใหม่

ประเภทของมัลแวร์

โฮคซ์ (Hoaxes)

โดยทั่วไปโฮคซ์ (Hoaxes) หมายถึง โปรแกรมที่เขียนขึ้นเพื่อหลอกให้ผู้ใช้ทำบางอย่างให้ โดยโฮคซ์จะใช้เทคนิคทางด้านวิศวกรรมสังคม (Social Engineering) เพื่อหลอกลวงให้ผู้ใช้งานคอมพิวเตอร์ อย่างไรก็ตามในกรณีนี้ โฮคซ์ไม่มีส่วนที่เป็นโค้ดประสงค์ร้ายใดๆ นอกจากแค่ต้องการหลอกเท่านั้น โฮดซ์มีหลากหลายแบบ แบบที่เห็นบ่อย เช่น การส่งอีเมลเพื่อหลอกว่ามีไวรัสตัวใหม่กำลังแพร่ระบาด และหลอกให้ส่งเมลนี้ต่อไปยังเพื่อนคนอื่นๆ ต่อ โฮคซ์ประเภทนี้ทำให้ผู้ใช้เสียเวลา ใช้รีซอร์สของเมลเซิร์ฟวอร์และใช้แบนด์วิธของเครือข่ายโดยเปล่าประโยชน์

ประเภทของมัลแวร์

สแกมส์ (Scams)

สแกมส์ (Scams) หมายถึง การใช้ช่องการสื่อสาร โดยอาชญากรเพื่อพยายามจะหลอกให้คนอื่นช่วยเหลือตัวเองในการทำอาชญากรรมบนอินเทอร์เน็ต เว็บไซต์และอีเมลอาจถูกใช้เพื่อหลอกคนอื่น ยกตัวอย่างเช่น ผู้ร้ายอาจใช้อีเมลเพื่อหลอกให้ผู้ใช้เปิดเผยข้อมูลส่วนตัว เช่น บัญชีธนคาร หมายเลขบัตรเครดิต แล้วอาชญากรอาจใช้ข้อมูลนี้เพื่อทำในสิ่งที่ผิดกฎหมาย สแกมส์ประเภทนี้ส่วนใหญ่จะเรียกว่า ฟิชชิง (Phishing) หรือแบรนด์สปู๊ฟฟิง (Brand Spoofing)หรือคาร์ดดิง (Carding)

ประเภทของมัลแวร์

สแปม (Spam)

สแปม (Spam) คือ การส่งอีเมลไปยังผู้ใช้จำนวนมาก โดยมีจุดประสงค์เพื่อการโฆษณาสินค้าหรือบริการ สแปมจัดอยู่ในประเภทสิ่งที่ก่อให้เกิดความรำคาญ แต่ไม่ใช่มัลแวร์เพราะไม่มีจุดประสงค์ร้าย อย่างไรก็ตามการส่งสแปมเมลจำนวนมหาศาลในปัจจุบันได้สร้างความเสียหาย เนื่องจากสแปมทำให้ผู้ใช้หรือพนักงานเสียเวลา เนื่องจากต้องลบอีเมลขยะทุกวัน

ประเภทของมัลแวร์

สปายแวร์ (Spyware)

สปายแวร์ (Spyware) บางทีก็รู้จักกันในชื่อ สปายบอต (Spybot) หรือแทร็คกิ้งซอฟต์แวร์ (Tracking Software) สปายแวร์เป็นโปรแกรมที่ใช้บางอย่างเพื่อลวงตา แต่ทำกิจกรรมบางอย่างในเครื่องคอมพิวเตอร์โดยที่ไม่ได้รับความยินยอมจากผู้ใช้ กิจกรรมต่งๆ ที่สปายแวร์ทำ เช่น การเก็บข้อมูลส่วนตัวของผู้ใช้ การปรับเปลี่ยนค่าที่กำหนดไว้ของบราวเซอร์นอกจากจะสร้างความรำคาญแล้ว ผลกระทบของสปายแวร์อาจมีตั้งแต่การลดประสิทธิภาพโดยรวมของคอมพิวเตอร์ไปจนถึงการละเมิดสิทธิส่วนบุคคลของผู้ใช้

ประเภทของมัลแวร์

แอดแวร์ (Adware)

แอดแวร์ (Adware) เป็นโปรแกรมโฆษณาสินค้าซึ่งจะเปิดป๊อบอัพวินโดวส์ แอดแวร์ส่วนใหญ่จะรวมอยู่ในบางแอพพลิเคชันที่ให้ใช้ได้ฟรี และจะฝังตัวอยู่เนื่องจากได้รับความยินยอมจากผู้ใช้ เนื่องจากแอดแวร์จะติดตั้งก็ต่อเมื่อผู้ใช้ได้ยินยอมตามข้อตกลงเกี่ยวกับลิขสิทธิ์ ดังนั้น จึงไม่ใช่โปรแกรมที่ผิดกฎหมาย อย่างไรก็ตามการป๊อบอัพวินโดวส์เพื่อโฆษณาสินค้าบางทีก็อาจสร้างความรำคาญให้กับผู้ใช้ได้ หรือบางกรณีอจทำให้ประสิทธิภาพของเครื่องลดลงได้นอกจากนี้ข้อมูลที่บางโปรแกมประเภทนี้เก็บรวบรวม ก็อาจจัดอยู่ในการละเมิดสิทธิส่วนบุคคลของผู้ที่ไม่ได้ให้ความสนใจต่อข้อตกลงที่เขียนไว้ก็ได้

ประเภทของมัลแวร์

มัลแวร์เรียกค่าไถ่ (Ransomware)

โปรแกรมมัลแวร์ที่เข้ารหัสข้อมูลของคุณ และถือเอาข้อมูลที่มีค่าเป็นตัวประกัน โดยรอการชำระเงินดิจิทัล ซึ่งเป็นจำนวนเปอร์เซ็นต์ที่เพิ่มขึ้นอย่างมากของมัลแวร์ในช่วงไม่กี่ปีที่ผ่านมา และเปอร์เซ็นต์ยังคงเพิ่มขึ้นอย่างต่อเนื่อง มัลแวร์เรียกค่าไถ่นั้น มักเลือกหน่วยงานที่เป็นเป้าหมายต่างๆ ที่เป็นสถานที่สำคัญๆ เช่น โรงพยาบาล สถานีตำรวจหรือแม้แต่องค์กรที่สำคัญในเมืองก็ตาม

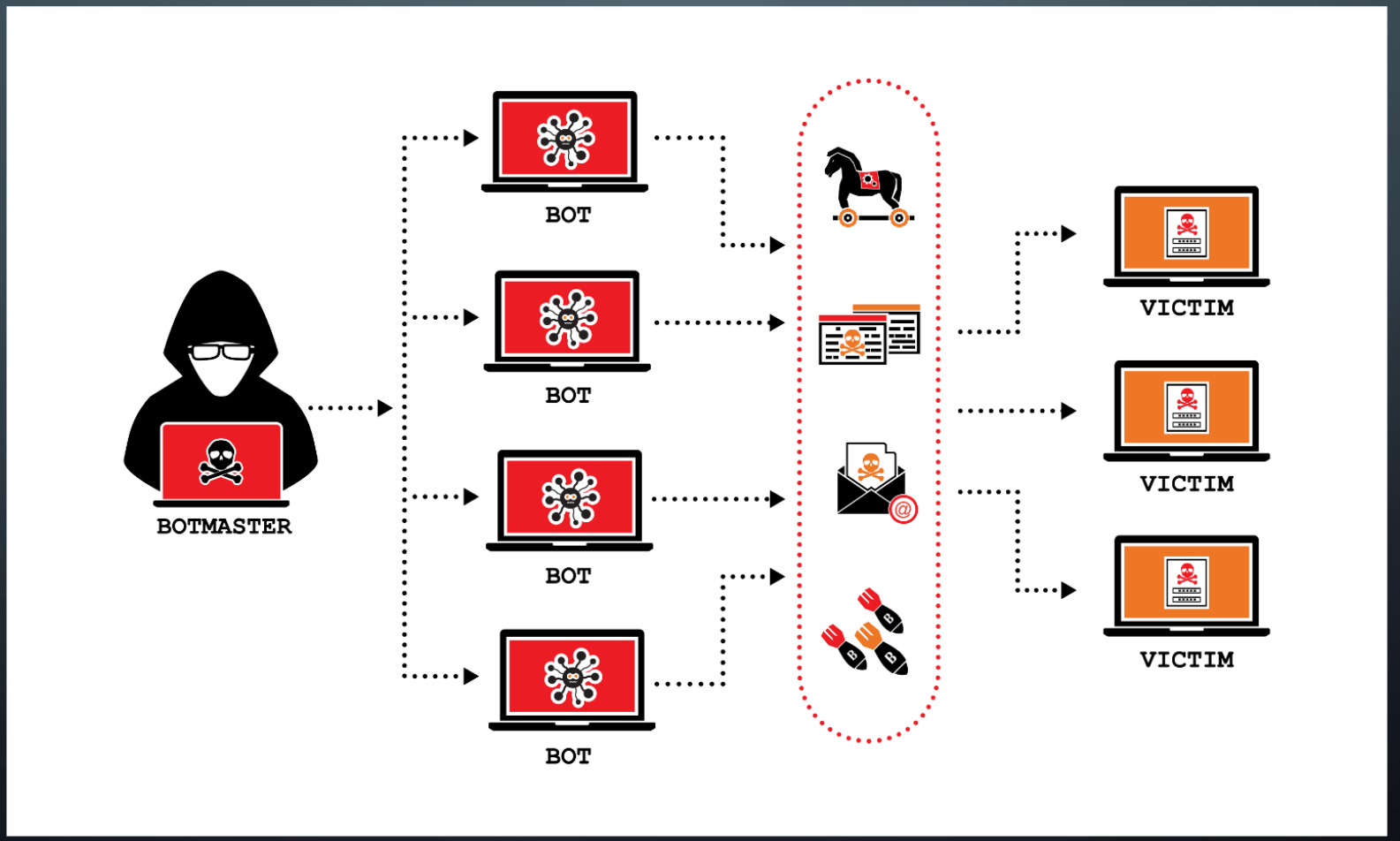
ประเภทของมัลแวร์

บอทเน็ต (Botnet)

Botnetเป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์ IoT อื่นๆ ในบ้านของเรา เพื่อรอรับคำสั่งจากแฮ็กเกอร์ โดยแฮ็กเกอร์จะนำ Botnet ที่มีไปใช้ในแคมเปญการโจมตีขนาดใหญ่ เช่น DDoS อย่างกรณีของ Mirai Botnet ที่โด่งดังเมื่อ 2 ปีก่อนซึ่งใช้ Botnet กว่า 300,000 เครื่องในการถล่มระบบของ Netflix, Twitter หรือ Reddit

ประเภทของมัลแวร์

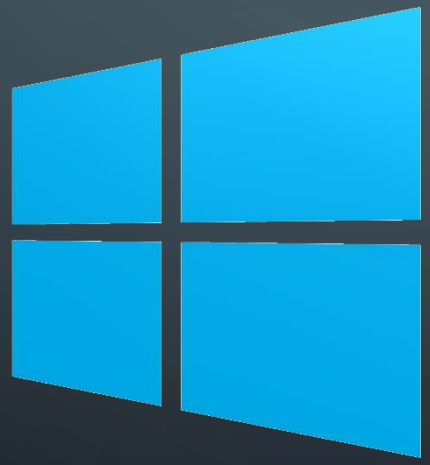
บอทเน็ต (Botnet)



คุณสมบัติของมัลแวร์

คุณสมบัติของเป้าหมาย

ประเภทของอุปกรณ์ : มัลแวร์บางตัวจะตั้งเป้าหมายไปที่อุปกรณ์เฉพาะบางอย่าง เช่น คอมพิวเตอร์ที่เป็นระบบวินโดวส์ หรือ XOS



คุณสมบัติของมัลแวร์

คุณสมบัติของเป้าหมาย

ระบบปฏิบัติการ : มัลแวร์อาจสามารถรันได้กับเฉพาะระบบปฏิบัติการหนึ่งเท่านั้น ยกตัวอย่างเช่น ไวรัส CIH หรือ Chernoby ที่แพร่ในปี 1990 จะโจมตีเฉพาะคอมพิวเตอร์ที่รันวินโดวส์ 95 และ 98 เท่านั้น

คุณสมบัติของมัลแวร์

คุณสมบัติของเป้าหมาย

แอพพลิเคชัน : มัลแวร์อาจต้องอาศัยแอพพลิดชันบางตัว เพื่อช่วยทำให้สามารถติดได้ เช่น ไวรัส LFM.926ในปี 2002 สามาถโจมตีได้กับเฉพาะโปรแกรม Shockwave Flash (.swf) เท่านั้น

คุณสมบัติของมัลแวร์

พาหะนำมัลแวร์

Executable file : เป้าหมายนี้เป็นเป้าหมายคลาสสิกหรือดั้งเดิม ไวรัสสามารถแพร่กระจายโดยการฝังตัวเองไปกับโปรแกรมอื่น นอกเหนือจากไฟล์ที่สามารถเอ็กเซ็กคิวต์ได้ ซึ่งจะมีนามสกุลเป็น .exe แล้วไฟล์อื่นที่สามารถรันได้ เช่น com, sys, dll, ovl, ocx และ .prg ก็สามารถรันได้เช่นกัน

คุณสมบัติของมัลแวร์

พาหะนำมัลแวร์

Script : การโจมตีนี้อาศัยภาษาสคริปต์เพื่อรันและทำให้ติดไวรัส ซึ่งภาษาสคริปต์ที่ว่านี้ เช่น Visual Basic, JavaScript, AppleScript เป็นต้น

คุณสมบัติของมัลแวร์

พาหะนำมัลแวร์

Macros : มาโครเป็นภาษาสดริปต์ของแอพพลิคชันบางตัว เช่น ไมโครซอฟท์ออฟฟิศ มัลแวร์จะอาศัยการรันมาโครสคริปต์นี้ในการแพร่กระจาย หรือติดต่อไปยังไฟล์อื่นหรือระบบอื่น หรือทำอันตรายให้กับระบบที่ติด เช่น ไวรัสสามารถใช้ภาษามาโครของไมโครซอฟท์เวิร์ด หรือ Lotus Ami Po เพื่อสร้างผลกระทบให้กับระบบหอโปรแกรมในรูปแบบต่างๆ เช่น การเปลี่ยนคำบางคำ หรือการเปลี่ยนสี หรือบางทีอาจจะฟอร์แมตฮาร์ดดิสก์ก็ได้

คุณสมบัติของมัลแวร์

พาหะนำมัลแวร์

Boot Sector : พื้นที่บางส่วนของฮาร์ดดิสก์หรือ CD-ROM เช่น MBR (Master Boot Record) หรือ DOS Boot Record อาจเป็นเป้าหมายก็ได้ เนื่องจากส่วนนี้สามารถรันโค้ดได้เมื่อดิสก์ติดไวรัสในส่วนนี้แล้ว การแพร่กระจายก็สามารถคิดขึ้นได้เมื่อดิสก์นี้ใช้สำหรับตระบบอื่น ถ้าไวรัสนั้นสามารถติดได้ทั้งไฟล์ทั่วไปและบู๊ตซ็กเตอร์ ไวรัสประเภทนี้เรียกว่า มัสติพารีไทต์ไวรัส (Multipartite Virus)

คุณสมบัติของมัลแวร์

กลไกการแพร่กระจายมัลแวร์

Removable media : การแพร่กระจายแบบดั้งเดิมของไวรัสและแบบที่เกิดขึ้นมากที่สุดคือ การก็อปปี้ไฟล์กลไกนี้เริ่มจากการใช้แผ่นฟล็ปปี้ดิสก์ หลังจากนั้นก็เปลี่ยนมาเป็นเครือข่าย และปัจจุบันมันกำลังมองหาช่องทางใหม่ เช่น USB (Universal Serial Bus) อย่างไรก็ตามอัตราการแพร่กระจายโดยอาศัยมีเดียต่างๆ นี้ยังเป็นได้ไม่เร็วเท่ากับการแพร่กระจายโดยอาศัยเครือข่ายคอมพิวเตอร์ นอกจากนี้ความเสี่ยงในการติดนั้นยังมีอยู่เสมอ เนื่องจากเป็นการยากที่จะป้องกันได้ร้อยเปอร์เซ็นต์ เพราะระบบยังคงต้องมีการแลกเปลี่ยนไฟล์กันอยู่เสมอ

คุณสมบัติของมัลแวร์

กลไกการแพร่กระจายมัลแวร์

Network share : เมื่อคอมพิวเตอร์ถูกเชื่อมต่อเข้ากับเครือข่ายก็จะมีการแชร์ไฟล์กันเพื่อความสะดวกในการแลกเปลี่ยนไฟล์ ซึ่งการแชร์ไฟล์ผ่านเครือข่ายนี้ก็กลายเป็นอีกช่องทางหนึ่งที่มัลแวร์ใช้ในการแพร่กระจายตัวเอง อีกทั้งการแพร่กระจายก็เป็นไปอย่างรวดเร็ว ถ้าเครือข่ายไม่มีระบบป้องกันและรักษาความปลอดภัยที่ดีการแชร์ไฟล์ผ่านเครือข่าย ก็อาจทำให้การแพร่กระจายมัลแวร์ไปยังคอมพิวเตอร์จำนวนมากได้ในเวลาอันรวดเร็ว

คุณสมบัติของมัลแวร์

กลไกการแพร่กระจายมัลแวร์

Network scanning : มัลแวร์อาจใช้เทคนิคนี้ในการสแกนเครือข่าย เพื่อค้นหาระบบที่มีจุดอ่อนหรือช่องโหว่และโจมตี ยกตัวอย่างเช่น กลไกนี้อาจส่งแพ็กก็ตที่สามารถเจาะเข้าระบบที่มีช่องโหวผ่านทางพอร์ตเฉพาะเพื่อค้นหาหรือทดสอบว่ามีระบบใดบ้างที่มีจุดอ่อนหรือช่องโหว่อยู่

คุณสมบัติของมัลแวร์

กลไกการแพร่กระจายมัลแวร์

peer-to-peer networks : หลักการทำงานของเพียร์ทูเพียร์เน็ตเวิร์คคือ เครื่องสองเครื่องใดๆ ที่ต้องการแชร์ข้อมูลหรือไฟล์และโฟลเดอร์ แต่ละเครื่องจะต้องติดตั้งโปรแกรมไคลเอนต์ โดยแต่ละเครื่องจะใช้การสื่อสารผ่านพอร์ตใดพอร์ตหนึ่ง เช่น พอร์ต 6,800-6,900 เป็นต้น แต่ถ้าองค์กรมีไฟล์วอลล์ผู้ดูแลระบบอาจจะไม่อนุญาตการสื่สารผ่านพอร์ตนี้ได้ อย่างไรก็ตามโปรแกรมเหล่านี้อาจสามารถกำหนดให้ใช้พอร์ตที่เปิดใช้งานอยู่แล้ว และนั่นก็อาจเป็นช่องทางในการแพร่กระจายไวรัสหรือมัลแวร์ก็ได้

คุณสมบัติของมัลแวร์

กลไกการแพร่กระจายมัลแวร์

E-mail : อีเมลกลายเป็นทางเลือกที่นิยมของการแพร่กระจายมัลแวร์ในปัจจุบัน เนื่องจากเป็นวิธีการที่ง่ายและคนส่วนใหญ่ก็ใช้อีเมลในการสื่อสารกับผู้ใช้คนอื่น ผ่านทางเครือข่ายและอินเทอร์เน็ตอยู่แล้ว โดยการใช้วิศวกรรมสังคมหรือใช้จิตวิทยา ทำให้ผู้ใช้อีเมลเปิดไฟล์ที่แนบมาด้วยได้ง่าย ดังนั้น การแพร่กระจายที่รวดเร็วและทำลายคอมพิวเตอร์จำนวนมากในปัจจุบัน จะใช้อีเมลเป็นสื่อในการแพร่กระจายมากที่สุด

คุณสมบัติของมัลแวร์

กลไกการแพร่กระจายมัลแวร์

Remote exploit : มัลแวร์อาจพยายามใช้ช่องโหว่ เพื่อแพร่กระจายตัวเอง พฤติกรรมอย่างนี้มักพบกันมากสำหรับมัลแวร์ประเภทเวิร์ม เช่นสแลมเมอร์เวิร์ม (Slammer worm) ใช้ประโยชน์จากช่องโหวในไมโครซอฟท์ SQL Server 2000 เวิร์มนี้จะทำให้เกิดบัฟเฟอร์โอเวอร์รัน (Buffer Overun) จนทำให้มันสามารถเขียนโค้ดลงบนบางส่วนของเมมโมรีของระบบ ซึ่งโค้ดส่วนนี้สมารถรันตัวเองได้เหมือนกับเป็นเซอร์วิสของ SQL Server บัฟเฟอร์โอเวอร์รันหมายถึง สภาพที่เกิดจากการป้อนข้อมูลข้าไปในบัฟฟอร์ มากกว่าที่บัฟเฟอร์นั้นจะสามารถรองรับได้แฮคเกอร์มักนิยมใช้เทคนิคนี้ในการเจาะเข้าควบคุมระบบไมโครซอฟท์ได้ใช้เวลาหลายเดือนในการแก้ไขหรือปิดช่องโหว่นี้หลังจากทีสแลมเอร์ออกมาโจมตี

คุณสมบัติของมัลแวร์

สื่อที่ใช้สำหรับแพร่ระบาดมัลแวร์

เครือข่ายภายนอก : ส่วนของเครือข่ายที่ไม่ได้อยู่ภายใต้การควบคุมขององค์กร ควรจัดว่าเป็นพื้นที่เสี่ยงที่อาจถูกโจมตี หรือเป็นแหล่งที่มาของการโจมตีได้ เนื่องจากอินเทอร์เน็ตเป็นระบบเปิดที่อาจมีใครก็ได้ที่มีจุดประสงคงร้าย และเป็นแหล่งที่สามารถเรียนรู้วิธีการใช้มัลแวร์ เพื่อโจมตีเป้าหมายได้หลากหลายรูปแบบ

คุณสมบัติของมัลแวร์

สื่อที่ใช้สำหรับแพร่ระบาดมัลแวร์

คอมพิวเตอร์ของแขกที่มาเยือน : ในขณะที่ความนิยมในการใช้โน้ตบุ๊ค อุปกรณ์อิเล็กทรอนิกส์แบบพกพาอื่นๆ เพิ่มขึ้นเรื่อยๆ อุปกรณ์เหล่นี้ต้องเคลื่อนย้ายเข้าออกองค์กรเป็นประจำ ถ้าอุปกรณ์เหล่านี้ไม่มีระบบป้องกันไวรัสที่ดี ก็อาจป็นแหล่งที่มาของการแพร่กระจายของไวรัสได้

คุณสมบัติของมัลแวร์

สื่อที่ใช้สำหรับแพร่ระบาดมัลแวร์

ไฟล์เอกสาร : ในขณะที่โปรแกรมเวิร์ดโพรเซสชอร์และสเปรดชีสมีความสามารถมากขึ้นเรื่อยๆ แต่ก็กลายเป็นเป้าหมายของการโจมตี โดยเฉพาะมาโครที่รองรับโดยแอพพลิเคชันเหล่านี้ เป็นจุดอ่อนที่ทำให้สามารถทำให้รันไวรัสหรือมัลแวร์ได้

คุณสมบัติของมัลแวร์

สื่อที่ใช้สำหรับแพร่ระบาดมัลแวร์

มีเดียเก็บข้อมูล : การถ่ายโอนไฟล์ผ่านทางอุปกรณ์จัดเก็บข้อมูลที่ถอดเข้าออกได้ก็อาจเป็นช่องทางหนึ่งของการแพร่กระจายไวรัสหรือมัลแวร์ได้

คุณสมบัติของมัลแวร์

เพย์โหลด (Payload)

Payload ของมัลแวร์ คือ **ส่วนของมัลแวร์ที่ทำหน้าที่หลักในการสร้างความเสียหาย** หรือดำเนินการตามวัตถุประสงค์ของผู้โจมตี หลังจากที่มัลแวร์สามารถแทรกซึมเข้าสู่ระบบเป้าหมายได้สำเร็จ

Payload เปรียบเสมือน "หัวใจสำคัญ" ของมัลแวร์ที่ถูกออกแบบมาเพื่อทำสิ่งต่าง ๆ ตามเจตนาของผู้สร้าง ซึ่งอาจเป็นการขโมยข้อมูล ทำลายระบบ แอบสอดแนม หรืออื่น ๆ

คุณสมบัติของมัลแวร์

เพย์โหลด (Payload)

Backdoor : เพย์โหลดประเภทนี้จะเปิดช่องโหว่ เพื่อให้แฮคเกอร์สามารถเข้ามาใช้งานระบบได้ ซึ่งอาจทำให้แฮคเกอร์สามารถควบคุมระบบได้ หรืออาจเป็นแค่การสร้าง FTP เซิร์ฟเวอร์ให้สามารถถ่ายโอนไฟล์ผ่านทางพอร์ต 21 ได้ หรืออาจเป็นการเปิด Telnet เพื่อเป็นฐานในการโจมตีเครื่องอื่นได้ อย่างที่ได้เคยกล่าวไว้ก่อนหน้าแล้วว่า แบ็คดอร์นั้นบางที่การเรียกว่าเป็นโทรจันฮอร์สประเภท RAT (Remote Access Trojan)

คุณสมบัติของมัลแวร์

เพย์โหลด (Payload)

Data Corruption or Deletion : หนึ่งในเพย์โหลดที่ทำให้มัลแวร์สามารถทำลายเครื่องที่ติดมากที่สุดคือการลบหรือทำลายไฟล์ข้อมูล หรือทำให้ไฟล์นั้นใช้งานไม่ได้ นักพัฒนามัลแวร์มีทางเลือกอยู่สองทางเลือกทางเลือกแรกคือ การทำให้เพย์โหลดถูกเอ็กเซ็กคิวต์ให้เร็วที่สุด เพื่อทำลายเครื่องที่ติดไวรัสนั้น ทำให้ยากต่อการป้องกันการแพร่กระจายของมัน อีกทางเลือกหนึ่งคือ การปล่อยเพย์โหลดทิ้งไว้ในเครื่องที่ติดในรูปแบบของโทรจันฮอร์สเพื่อเอ็กเซ็กคิวต์ในเวลาต่อมา ทำให้มีช่วงเวลาสำหรับการตรวจจับมัลแวร์ประเภทนี้ได้

คุณสมบัติของมัลแวร์

เพย์โหลด (Payload)

Information Theft : มัลแวร์อีกประเภทหนึ่งที่สร้างความกังวลให้กับผู้ใช้งานเครื่องคือ มัลแวร์ที่ออกแบบมาสำหรับการขโมยข้อมูลที่สำคัญจากระบบที่ติดมัลแวร์ ถ้ามัลแวร์สามารถหลีกเลี่ยงหรือทำลายระบบซีเดียวริตี้ของเครื่องได้ มัลแวร์ประเภทนี้จะสามารถขโมยและส่งข้อมูลกลับไปยังแฮคเกอร์ได้

คุณสมบัติของมัลแวร์

เพย์โหลด (Payload)

Denial of Service (DoS) : หนึ่งในเพย์โหลดที่ทำได้ง่ายและพบเห็นทั่วไปคือการโจมตีแบบปฏิเสธการให้บริการหรือ DoS การโจมตีแบบนี้คือ การทำให้เครื่องที่ถูกโจมตีโอเวอร์โหลดหรือหยุดให้บริการ เช่น เว็บเซิร์ฟวอร์หรือเมลเซิร์ฟเวอร์ DoS มีจุดประสงค์เพื่อทำให้เซอร์วิสบางตัวไม่สามารถให้บริการได้ในช่วงเวลาหนึ่ง

คุณสมบัติของมัลแวร์

เพย์โหลด (Payload)

Distributed Denial of Service (DDoS) : การโจมตีแบบ DDoS คือ การใช้เครื่องไคลเอนต์หลายๆเครื่องช่วยกันโจมตีครื่องที่เป็นเป้าหมายเครื่องหนึ่ง การทำอย่างนี้ก็เพื่อเพิ่มความรุนแรงในการโจมตีเนื่องจากการโจมตีจากหลายเครื่อง มักจะทำความเสียหายได้มากกว่าการใช้เครื่องเดียวในการโจมตีหนึ่งครั้ง จะส่งข้อมูลหรือแพ็กเก็ตจำนวนมากๆ ไปยังเครื่องเป้าหมายจนทำให้ไม่สามารถรองรับแพ็กเก็ตจำนวนมหาศาลนี้ได้ และทำให้เครื่องนั้นไม่สมารถให้บริการได้ ซึ่งการทำเช่นนี้เป็นการฟลัดแบนด์วิธ (Flood bandwidth)ของเครือข่าย หรือการใช้แบนด์วิธให้หมดเพื่อจะได้ไม่ให้คนอื่นสามารถใช้ได้ การโจมตีแบบนี้เป็นการโจมตีที่ยากต่อการป้องกันเนื่องจากโฮสต์ที่ใช่โจมตีนั้น ส่วนใหญ่เป็นโฮสต์ที่ถูกโจมตีหรือเจาะเข้าไป เพื่อฝังโปรแกรมที่ใช้สำหรับโจมตีอีกทีหนึ่ง DDoS ส่วนใหญ่จะเกิดจากการใช้โปรแกรมบอต (Bots) ซึ่งเป็นโปรแกรมที่ทำหน้าที่บางอย่างอัตโนมัติ เช่น เอ็กกดรอป (Eggdrop)เป็นบอตหนึ่งที่แฮคเกอร์ใช้สำหรับควบคุมคอมพิวเตอร์ผ่านทางช่องทาง IRC (Internet Relay Chat) เมื่อคอมพิวเตอร์นั้นถูกควบคุมได้แล้วเครื่องนั้นก็จะกลายเป็นซอมบี้ส์ (Zombies) ซึ่งแฮคเกอร์สามารถส่งคำสั่งให้เครื่องนี้ทำงานบางอย่าง โดยที่ผู้ที่เป็นเจ้าของเครื่องนั้นอาจไม่รู้ตัว

คุณสมบัติของมัลแวร์

เพย์โหลด (Payload)

Network DoS : เพย์โหลดประเภทนี้จะพยายามที่จะโอเวอร์โหลดรีซอร์สของเครื่องที่ถูกโจมตี เช่นโพรเซสเซอร์ เมมโมรี เป็นต้น ซึ่งส่วนใหญ่จะถูกโจมตีแบบ SYN Flood โดยแฮคเกอร์จะใช้โปรแกรมสำหรับส่งแพ็กเก็แบบ TCP SYN เพื่อไปทำให้คิว (QUEUE) หรือบัฟเฟอร์ของเครื่องนั้นเต็ม ทำให้ผู้ใช้ทั่วไปไม่สามารถใช้บริกรนั้นได้ E-mal Bomb ก็เป็นการโจมตีหนึ่งที่ทำให้พื้นที่เก็บเมลเต็ม โดยการส่งเมลที่มีขนาดใหญ่มากไปยังที่อยู่อีเมลหนึ่งเพื่อทำให้เมลหยุดทำงานหรือไม่สามารถรับเมลจากที่อื่นได้อีก

คุณสมบัติของมัลแวร์

เพย์โหลด (Payload)

System shutdowns : การทำให้เครื่องที่ถูกโจมตีถูกชัตดาวน์หรือล่มได้นั้น สามารถทำได้โดยการทำลายเซอร์วิสของระบบหนึ่งเซอร์วิสหรือมากกว่า การโจมตีประเภทนี้มัลแวร์จะค้นหาช่องโหว่หรือจุดอ่อนของแอพพลิเคชันหรือระบบปฏิบัติการ ซึ่งทำให้ระบบชัตดาวน์ลงได้

คุณสมบัติของมัลแวร์

เพย์โหลด (Payload)

Bandwidth flooding : เซอร์วิสส่วนใหญ่ที่ให้บริการจะใช้ช่องการเชื่อมต่อเข้ากับเครือข่าย ซึ่งช่องนี้จะมีข้อจำกัดเกี่ยวกับอัตราการถ่ายโอนข้อมูลหรือแบนด์วิธ ถ้ามัลแวร์สามารถส่งแพ็กเก็ตจนเต็มช่องแบนด์วิธนี้ได้ ผู้ใช้ทั่วไปก็จะไม่สามารถข้ามาใช้เซอร์วิสนี้ได้เนื่องจากแบนด์วิธถูกใช้ไปหมดแล้ว

คุณสมบัติของมัลแวร์

เพย์โหลด (Payload)

Service disruption : เพย์โหลดประเภทนี้อาจทำให้เกิด DoS ได้ ยกตัวอย่างเช่น ถ้าการโจมตี DNS เซิร์ฟเวอร์ ทำให้เครื่องนั้นไม่สามารถให้บริการ DNS ก็เป็นการโจมตีแบบ DoS ได้เช่นกัน ถึงแม้ว่าบริการอื่นยังคงใช้งานได้ตามปกติ แต่บริการอื่นที่ว่านี้อาจต้องศัย DNS ไคลเอนต์จึงจะสามารถใช้บริการนี้ได้เช่น เว็บ เมล เป็นต้น

คุณสมบัติของมัลแวร์

การจุดชนวน

Manual execution : การจุดชนวนประเภทนี้คือ การที่ผู้ใช้รันโปรแกรมที่เครื่องโดยตรง ซึ่งอาจจะทำโดยไม่รู้ตัวหรือเป็นการหลอกให้รันโปรแกรม โดยอาจใช้วิธีวิศวกรรมสังคมหรือจิตวิทยา มัลแวร์โดยทั่วไปจะใช้บางรูปแบบของวิศวกรมสังคม ในการหลอกให้ผู้ใช้รันโปรแกรมมัลแวร์เหล่านั้นเอง วิธีนี้เป็นวิธีที่ง่ายมากตัวอย่างเช่น ไวรัสที่ใช้อีเมลป็นสื่อในการแพร่กระจาย โดยไวรัสจะสร้างหัวข้อเรื่องของเมลที่ทำให้น่าสนใจต่อผู้อนเพื่อให้เปิดเมลนั้น หรือการสปู๊พฟิง (Spoofing) อีเมลเพื่อให้ผู้รับเชื่อว่าอีเมลนั้นมาจากแหล่งที่เชื่อถือได้

คุณสมบัติของมัลแวร์

การจุดชนวน

Semi-automatic execution : การจุดชนวนประเภทนี้เริ่มจากการที่ผู้ใช้รันโปรแกรมมัลแวร์เองแล้วหลังจากนั้นโปรแกรมก็จะทำงานต่อโดยอัตโนมัติ

Automatic execution : มัลแวร์ประเภทนี้จะรันตัวมันเองโดยอัตโนมัติโดยไม่ต้องอาศัยผู้ใช้

คุณสมบัติของมัลแวร์

การจุดชนวน

Time bomb : การจุดชนวนประเภทนี้มัลแวร์จะรันเมื่อช่วงระยะเวลาหนึ่งหลังจากที่เครื่องติดไวรัสแล้วหรือในวันเวลาใดเวลาหนึ่ง ยกตัวอย่างเช่น เวิร์มมายดูมดอดบี (MyDoom.B Worm) ได้เริ่มรันเพย์โหลดเพื่อโจมตีเว็บไซต์ของไมโครซอฟท์ (www.microsoft.com) เฉพาะวันที่ 3 กุมภาพันธ์ 2004 และโจมตีเว็บไซต์ของ SCO Group ในวันที่ 1 กุมภาพันธ์ 2004

คุณสมบัติของมัลแวร์

การจุดชนวน

Conditional : การจุดชนวนประเภทนี้เริ่มโดยเมื่อสภาพแวดล้อมตรงตามเงื่อนไขที่กำหนด ยกตัวอย่าง เช่น เมื่อมีการเปลี่ยนชื่อไฟล์ เมื่อมีการกดปุ่มคีย์บอร์ดบางคีย์ หรือเมื่อเปิดบางโปรแกรม มัลแวร์ประเภทนี้บางที่ก็เรียกว่า ลอจิกบอมบ์ (Logic Bomb)

คุณสมบัติของมัลแวร์

กลไกการป้องกันตัวเองของมัลแวร์

Armor : เทคนิคการป้องกันประเภทนี้จะพยายามและป้องกันการวิเคราะห์โค้ดของมัลแวร์ เช่น มัลแวร์จะตรวจดูว่าโปรแกรมดีกบัคเกอร์ (Debugger) กำลังรันอยู่หรือไม่ และป้องกันหรือทำให้ดีบั๊กเกอร์ทำงานไม่ถูกต้อง หรือการเพิ่มโค้ดจำนวนมากที่ไม่มีความหมายใดๆ เพื่อทำให้ยากต่อการวิเคราะห์จุดมุ่งหมายของโค้ดมัลแวร์นี้

คุณสมบัติของมัลแวร์

กลไกการป้องกันตัวเองของมัลแวร์

Stealth : มัลแวร์ใช้เทคนิการซ่อนพรางตัวโดยการให้ข้อมูลที่ผิดๆ เมื่อโปรแกรมสแกนไวรัสพยายามจะสแกนมัลแวร์ ยกตัวอย่างเช่น ไวรัสบางตัวอาจจะบันทึกไฟล์หรืออิมเมจที่ยังไม่ติดไวรัสในบู๊ตเซ็กเตอร์เมื่อขณะมีการพยายามที่จะตรวจช็คว่า บู๊ตซ็กเตอร์ติดไวรัสหรือไม่ ไวรัสเก่าแก่อย่างเช่น เบรน (Brain Virus) ใช้เทคนิคนี้ในปี 1986

คุณสมบัติของมัลแวร์

กลไกการป้องกันตัวเองของมัลแวร์

Encryption : มัลแวร์บางประเภทจะใช้วิธีการเข้ารหัสโค้ดตัวเองและเพย์โหลด หรือบางทีอาจรวมทั้งข้อมูลระบบด้วยเพื่อป้องกันการตรวจพบ มัลแวร์ที่เข้ารหัสประกอบด้วยฟังก์ชั่นการเข้ารหัส คีย์ และโค้ดมัลแวร์ที่ถูกเข้ารหัสแล้ว เมื่อมัลแวร์ถูกรันแล้วก็จะใช้ฟังก์ชั่นการเข้ารหัสและคีย์เพื่อถอดรหัสโค้ดมัลแวร์ หลังจากนั้นมัลแวร์ก็จะก็อปปี้ตัวเองไปยังไฟล์ใหม่พร้อมทั้งสร้างคีย์ใหม่ขึ้นเพื่อเข้ารหัสตัวเองอีกครั้ง แล้วแนบคีย์และฟังก์ชั่นการเข้ารหัสไปกับมัลแวร์ที่เข้ารหัสแล้ว ซึ่งทำให้กลายเป็นก็อปขี้ใหม่ของมัลแวร์ มัลแวร์ประเภทนี้จะต่างจากไวรัสประเภทโพลิมอร์พิก เพราะมัลแวร์จะใช้ฟังก์ชั่นในการเข้ารหัสเดียวกันเสมอแต่คีย์จะถูกเปลี่ยนไปทุกครั้ง ซอฟต์แวร์ป้องกันไวรัสอาจตรวจเจอฟังก์ชันที่ใช้สำหรับเข้ารหัส และทำให้ตรวจเจอมัลแวร์ประเภทนี้ได้ง่ายกว่า

คุณสมบัติของมัลแวร์

วงจรชีวิตของมัลแวร์

การค้นพบช่องโหว่ : การพัฒนามัลแวร์นั้นส่วนใหญ่จะเริ่มเมื่อมีการค้นพบวิธีใหม่ๆ ในการโจมตี การค้นพบช่องโหว่หรือจุดอ่อนของบางโปรแกรม และได้มีการเผยแพร่ในสังคมของพวกแฮคเกอร์ ในช่วงนี้นักเขียนมัลแวร์ก็จะช่วยกันพัฒนาและค้นหาวิธีการที่จะใช้ประโยชน์จากจุดอ่อนหรือช่องโหว่นี้

คุณสมบัติของมัลแวร์

วงจรชีวิตของมัลแวร์

การพัฒนา : การเขียนมัลแวร์นั้นส่วนใหญ่จะต้องอาศัยความเข้าใจภาษาแอสเซมบลิ (Assembly Language) เข้าใจการทำงานของระบบคอมพิวเตอร์ที่จะโจมตี ปัจจุบันนั้นมีเครื่องมือที่ช่วยในการพัฒนามัลแวร์ได้ง่ายขึ้น ประกอบกับแหล่งความรู้และความช่วยเหลือจากอินเทอร์เน็ตนั้น ทำให้การพัฒนามัลแวร์นั้นเป็นเรื่องง่าย

คุณสมบัติของมัลแวร์

วงจรชีวิตของมัลแวร์

การแพร่ระบาด : หลังจากมัลแวร์ได้ถูกพัฒนาเสร็จแล้วได้ประกาศและปล่อยให้สาธารณะทราบ ส่วนใหญ่จะแพร่ระบาดไปยังโฮสต์ต่างๆ ที่จะโจมตีก่อน จากนั้นจะเริ่มทำลายระบบเมื่อพบเงื่อนไขการจุดชนวน ถึงแม้ว่าจะมีโปรแกรมมัลแวร์ที่เป็นที่รู้จักกันมากมาย แต่มีเพียงบางส่วนเท่านั้นที่ถูกปล่อยออกมาสู่สาธารณะไวรัสที่ถูกเขียนขึ้นนั้นส่วนใหญ่จะไม่ถูกปล่อยให้ออกสู่สาธารณะเลย ซึ่งไวรัสกลุ่มนี้เป็นที่รู้จักกันในนามสวนสัตว์ไวรัส (Zoo Viruses)

คุณสมบัติของมัลแวร์

วงจรชีวิตของมัลแวร์

การทำลาย : หลังจากที่มัลแวร์สามารถข้ามาในระบบแล้วขั้นตอนต่อไปคือ การปล่อยให้เพย์โหลดทำงานถ้าโค้ดเพย์โหลดถูกกำหนดให้รันตามงื่อนไข ช่วงนี้ก็อยู่ในช่วงของการรอให้เป็นไปตามเงื่อนไขนั้น ยกตัวอย่างเช่น เพย์โหลดของมัลแวร์บางประเภท จะถูกรันก็ต่อเมื่อผู้ใช้ได้ทำอะไรบางอย่าง หรือถึงวันเวลาที่กำหนด ส่วนมัลแวร์ที่ไม่ต้องมีเงื่อนไข ก็อาจปล่อยให้เพย์โหลดทำงานทันทีที่ระบบนั้นติดไวรัส ยกตัวอย่างเช่น เพย์โหลดที่เก็บล็อคการทำงานของระบบ เมื่อมัลแวร์ติดเครื่องนั้น เพย์โหลดก็จะทำงานทันทีเพื่อเก็บสะสมรวบรวมข้อมูลที่ต้องการ

คุณสมบัติของมัลแวร์

วงจรชีวิตของมัลแวร์

การตรวบพบและแจ้งเตือน : เมื่อเวลาผ่านไปช่วงหนึ่งบริษัทผู้ผลิตซอฟต์แวร์ป้องกันไวรัส ก็จะค้นพบมัลแวร์หรือไวรัสตัวใหม่นี้ ส่วนใหญ่นั้นขั้นตอนนี้อาจเกิดขึ้นก่อนขั้นตอนที่ 4 หรือ 3 แต่ก็ไม่เสมอไปช่วงนี้ก็เป็นช่วงเวลาที่จะหาทางป้องกันและตรวจจับไวรัสประเภทนี้

คุณสมบัติของมัลแวร์

วงจรชีวิตของมัลแวร์

การตรวจจับ : หลังจากที่ภัยจากมัลแวร์ได้ถูกปิดเผยแล้ว ซอฟต์แวร์ป้องกันไวรัสก็จะวิเคราะห์และพัฒนาโค้ดที่จะตรวจจับมัลแวร์นี้ หลังจากที่ค้นพบวิธีตรวจจับก็จะอัพเดตซิกเนเจอร์ เพื่อให้โปรแกรมป้องกันมัลแวร์ที่ใช้งานอยู่แล้วสมารถตรวจจับไวรัสตัวใหม่นี้ได้ด้วย ช่วงเวลานี้เป็นช่วงเวลาที่สำคัญที่จะช่วยในการควบคุมการโจมตีและแพร่ระบาดของไวรัสนี้ได้

คุณสมบัติของมัลแวร์

วงจรชีวิตของมัลแวร์

การป้องกันและกำจัด : หลังจากที่ไวรัสซิกเนเจอร์ได้เผยแพร่ต่อสาธารณะ ขั้นตอนต่อไปก็เป็นความรับผิดชอบของผู้ใช้คอมพิวเตอร์ที่จะต้องอัพเดตซิกเนเจอร์เป็นประจำ เพื่อป้องกันการโจมตี หรือกำจัดไวรัสตัวใหม่นี้ถ้าระบบนั้นได้ติดไวรัสนั้นแล้ว

มัลแวร์ที่มีชื่อเสียง

SQLSlammer

ชื่ออื่นที่รู้จัก :	Net-Worm.Win32.Slammer (Kaspersky Lab), Worm.SQL.Slammer (Kaspersky Lab), W32/SQLSlammer.worm (McAfee), W32.SQLExp.Worm.dump (Symantec), W32/SQLSlam-A (Sophos), Win32/SQLSlammer.worm (RAV), SQLSLAMMER.A (Trend Micro), Worm/SQL.Slammer.dmp (H+BEDV), SQLSlammer.A (FRISK), Win32:SQLSlammer (ALWIL), SQLSlammer (Grisoft), Win32.Worm.SQL.Slammer.A (SOFTWIN), W32/SQLSlammer (Panda), Win32/SQLSlammer.A.image (Eset)
พบครั้งแรกเมื่อ :	24 มกราคม 2003
ประเภท :	เวิร์ม
ระบบที่มีผลกระทบ :	Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me

มัลแวร์ที่มีชื่อเสียง

SQLSlammer

เป็นเวิร์มที่มีป้าหมายการโจมตีคือ ระบบที่รัน Microsoft SQL Server2000 และ Microsoft Desktop Engine (MSDE) 2000 โดยเวิร์มนี้จะส่งข้อมูลขนาด 376 ไบต์ไปยังพอร์ต 1434/UDP ซึ่งเป็นพอร์ตที่เปิดให้บริการโดย SQL Server ซึ่งจะทำให้เกิดบัฟเฟอร์โอเวอร์โฟลว์ ซึ่งทำให้บางส่วนของหน่วยความจำถูกเขียนทับ

มัลแวร์ที่มีชื่อเสียง

W32.Sasser.Worm

ชื่ออื่นที่รู้จัก :	W32/Sasser.worm.a [McAfee], WORM_SASSER.A [Trend], Worm.Win32.Sasser.a [Kaspersky], W32/Sasser-A [Sophos], Win32.Sasser.A [Computer Associates], Sasser [F-Secure], W32/Sasser.A.worm [Panda]
พบครั้งแรกเมื่อ :	30 เมษายน 2004
ประเภท :	เวิร์ม
ระบบที่มีผลกระทบ :	Windows 2000, Windows XP

มัลแวร์ที่มีชื่อเสียง

W32.Sasser.Worm

เมื่อ Win32/Sasser รันบนคอมพิวเตอร์ มันก็จะก็อปปี้ตัวเองไปไว้ที่โฟลเดอร์ %WINDOWS% และจะเพิ่มคีย์ในรีจิสทรี HKEY LOCAL MACHINE\Software\Microsoft\Windows\currentversion \Run ซึ่งจะทำให้เวิร์มเริ่มทำงานทันทีที่มีการสตาร์ทวินโดวส์ Win32/Sasser จะทำตัวเป็น FTP เซิร์ฟเวอร์โดยจะเปิดพอร์ต 5554 เพื่อรอรับการเชื่อมต่อจากภายนอกเมื่อมีการเชื่อมต่อข้ามา เวิร์มก็จะส่งก็ปปี้ตัวเองไปให้โฮสต์นั้น

มัลแวร์ที่มีชื่อเสียง

W32.Mydoom.BB@mm

ชื่ออื่นที่รู้จัก :	W32.Mydoom.BB@mm [Symantec], Email-Worm.Win32.Mydoom.am [Kaspersky Lab], W32/Mydoom.bf@MM [McAfee], W32/MyDoom-BE [Sophos], WORM_MY-DOOM.BE [Trend Micro]
พบครั้งแรกเมื่อ :	21 กุมภาพันธ์ 2005
ประเภท :	เวิร์ม
ระบบที่มีผลกระทบ :	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

มัลแวร์ที่มีชื่อเสียง

W32.Mydoom.BB@mm

MyDoom.BB ปรากฏครั้งแรกเมื่อวันที่ 17 ก.พ. 2005 เป็นเวิร์มที่จะส่งเมลจำนวนมาก โดยจะแนบตัวเองไปพร้อมกับเมลด้วย ส่วนหัวข้อเรื่องและเนื้อหาของเมลก็มีหลากหลาย ในส่วนเนื้อหาของเมลจะมีไฟล์เอ็กเซ็กคิวต์ได้ (Windows PE) ซึ่งจะถูกบีบอัดด้วย MEW executable compressor เวิร์มเวอร์ชันนี้เป็นเวอร์ชันที่มีการปรับปรุงจากเวอร์ชันก่อนหน้าคือ Mydoom.M

มัลแวร์ที่มีชื่อเสียง

W32.Netsky.B@mm

ชื่ออื่นที่รู้จัก :	W32.Netsky.B@mm [Symantec], W32/Netsky.b@MM [McAfee], W32/Netsky.B.worm [Panda], WORM_NETSKY.B [Trend Micro], Moodown.B [F-Secure], I-Worm.Moodown.b [Kaspersky], I-Worm.NetSky.b [Kaspersky], W32/Netsky-B [Sophos], Win32.Netsky.B [Computer Associates]
พบครั้งแรกเมื่อ :	18 กุมภาพันธ์ 2004
ประเภท :	เวิร์ม
ระบบที่มีผลกระทบ :	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows XP

มัลแวร์ที่มีชื่อเสียง

W32.Netsky.B@mm

W32.Netsky.B@mm สามารถแพร่กระจายผ่านทางอีเมลด้วยคอมโพเนนต์สำหรับการส่งอีเมลด้วยตัวเอง ผ่านโปรโตคอลชื่อ Simple Mail Transfer Protocol (SMTP) โดยอาศัยเครื่องที่ถูก worm ชนิดนี้คุกคาม เป็นพาหะสำหรับการส่งอีเมลที่แนบไฟล์ของ worm ชนิดนี้ออกมาในปริมาณมาก และอีเมลแอดเดรสที่ส่งไปนั้น worm จะสแกนหาในไฟล์ต่างๆ นอกจากนี้หนอนชนิดนี้ยังมีความสามารถในการแพร่กระจายตัวผ่านทางการแชรไฟล์ โดย worm จะค้นหาตั้งแต่ไดรว์ C: จนกระทั่งไดรว์ Z: ถ้าพบโฟลเดอร์ใดก็ตามที่มีชื่อประกอบด้วยคำว่า "Share" หรือ "Sharing” ก็จะคัดลอกตัว worm เองไปยังโฟลเดอร์นั้นๆ

มัลแวร์ที่มีชื่อเสียง

Win32/Conficker

ชื่ออื่นที่รู้จัก :	W32.Downadup, Win32/Conficker.A [Computer Associates], W32/Downadup.A [F-Secure], Conficker.A [Panda Software], Net-Worm.Win32.Kido.bt [Kaspersky], WORM_DOWNAD.AP [Trend], W32/Conficker [Norman]
พบครั้งแรกเมื่อ :	21 พฤศจิกายน 2008
ประเภท :	เวิร์ม
ระบบที่มีผลกระทบ :	Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000

มัลแวร์ที่มีชื่อเสียง

Win32/Conficker

Conficker หรือ Downandup หรือ Kido เป็น worm ที่แพร่กระจายตัวเองโดยโจมตีผ่านช่องโหว่ Windows Server service (SVCHOST.EXE) ของระบบปฏิบัติการไมโครซอฟท์วินโดวส์ เมื่อติด worm ชนิดนี้แล้ว สิ่งที่เกิดขึ้นคือ เครื่องแม่ข่ายที่ทำหน้าที่เป็นโดมนคอนโทรลลอร์ จะเกิดภาวะโอเวอร์โหลดคือ ไม่สามารถรองรับการเรียกใช้งานของเครื่องลูกข่ายได้ สืบเนื่องมาจาก worm ชนิดนี้จะสร้างคอนเน็กชันจำนวนมาก

มัลแวร์ที่มีชื่อเสียง

CryptoLocker

ชื่ออื่นที่รู้จัก :	Win32/Crilock.A
พบครั้งแรกเมื่อ :	2 มิถุนายน 2014
ประเภท :	โทรจันฮอร์ส, แรนซัมแวร์
ระบบที่มีผลกระทบ :	วินโดวส์

มัลแวร์ที่มีชื่อเสียง

CryptoLocker

คริพโตล็อกเกอร์ เป็นแรนซัมแวร์ (Ransomware) หรือมัลแวร์เรียกค่าไถ่บนระบบปฏิบัติการวินโดวส์ โดยถูกเผยแพร่ผ่านทางไฟล์แนบในอีเมลหลอกลวง เช่น อีเมลแจ้งการติดตามพัสดุจาก FedEx, UHS หรือ UPS พร้อมกับแนบไฟล์ ZIP ซึ่งภายในมีไฟล์ EXE ที่ถูกปลอมแปลงว่าเป็นไฟล์ PDF หรือผ่านทางมัลแวร์ประเภทบอตเน็ตที่เคยถูกติดตั้งลงบนเครื่องของผู้ใช้มาก่อน หลักการทำงานโดยทั่วไปของคริพโตล็อกเกอร์นั้นคล้ายคลึงกับแรนซัมแวร์ตัวอื่นๆ ในอดีตที่ผ่านมา นั่นคือเข้ารหัสลับข้อมูลไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ และไฟล์ประเภทอื่นๆ ในเครื่องคอมพิวเตอร์ของเหยื่อจากนั้นจะขึ้นข้อความข่มขู่ให้ผู้ใช้ชำระเงินภายในวลาที่กำหนด ก่อนที่ข้อมูลทั้งหมดจะไม่สามารถถูกถอดรหัสลับได้อีกตลอดไป ทั้งนี้ไม่ใช่เฉพาะข้อมูลในคอมพิวเตอร์ของเหยื่อเท่านั้นที่ถูกเข้ารหัสลับ แต่ข้อมูลที่แชร์ร่วมกันในระบบเครือข่ายก็ถูกเข้ารหัสลับด้วยเช่นกัน

แนวทางการป้องกันมัลแวร์

ติดตั้งโปรแกรมป้องกันมัลแวร์

แนวทางการป้องกันมัลแวร์

การลบโปรแกรมที่ไม่ได้ใช้งาน

ขั้นตอนแรกในการป้องกันคือ การลดช่องทางที่ไวรัสอาจจะใช้เป็นสื่อที่จะเข้ามาในเครื่อง ตัวอย่าง เช่น การลบแอพพลิเคชันหรือเซอร์วิสที่ไม่จำเป็นออกจากครื่อง ซึ่งเป็นกรลดจำนวนช่องทางที่แฮคเกอร์หรือไวรัสอาจใช้ประโยชน์ได้ บางระบบปฏิบัติการนั้นเมื่อติดตั้งโดยดีฟอลต์ อาจมีบางเซอร์วิสที่ไม่จำเป็นต้องใช้ เช่น เว็บเซิร์ฟเวอร์ FTP เซิร์ฟเวอร์และเมลเซิร์ฟเวอร์ เป็นต้น ซึ่งถ้าไม่จำเป็นต้องใช้ก็ไม่ควรติดตั้ง

แนวทางการป้องกันมัลแวร์

การอัพเดทแพทช์

แพทช์ซอฟต์แวร์แก้ไขข้อผิดพลาด แต่สามารถเผยแพร่เพื่อแก้ไขช่องโหว่ด้านความปลอดภัยและความไม่สอดคล้องกันในซอฟต์แวร์ได้ การข้ามผ่านการอัปเดตที่สำคัญเหล่านี้อาจทำให้คอมพิวเตอร์โทรศัพท์หรืออุปกรณ์อื่น ๆ ของคุณเปิดการโจมตีโดยมัลแวร์

แนวทางการป้องกันมัลแวร์

การสแกนจุดอ่อนของระบบ (Vulnerability Scan)

หลังจากที่ติดตั้งและคอนฟิกระบบแล้ว ควรจะมีการตรวจเช็คเป็นประจำเพื่อให้แน่ใจว่าไม่มีจุดอ่อนใดๆ ในระบบเพื่อช่วยให้กระบวนการนี้มีประสิทธิภาพ อาจใช้เครื่องมือในการสแกนจากหลายบริษัท เพื่อช่วยในการค้นหาจุดอ่อนและช่องโหว่ของระบบ โดยส่วนใหญ่เครื่องมือเหล่านี้จะอัพเดตตัวเอง เพื่อจะสามารถตรวจค้นหาจุดอ่อนหรือช่องโหวใหม่ๆในระบบ

แนวทางการป้องกันมัลแวร์

กำหนดสิทธิ์ของผู้ใช้งานระบบให้น้อยที่สุด

อีกส่วนหนึ่งที่สำคัญสำหรับการป้องกันครื่องไคลเอนต์คือ การกำหนดสิทธิ์ของผู้ใช้ที่ต้องใช้งานเป็นประจำให้มีสิทธิ์น้อยที่สุด หรือเพียงพอสำหรับการทำงานประจำของแต่ละคน เพื่อป้องกันไวรัสบางตัวที่พยายามจะใช้ประโยชน์จากสิทธิ์ของผู้ใช้ในการโจมตีหรือทำลายระบบ ตัวอย่างเช่น ผู้ดูแลระบบ (Administrator) มีสิทธิ์สูงสุดและสามารถทำอะไรได้ทุกอย่าง ดังนั้ จึงไม่ควรล็อกอินในฐนะผู้ดูแลระบบเพื่อทำงานทั่วไป ควรล็อกอินเฉพาะตอนที่จำเป็นในการดูแลระบบจริงๆ เท่านั้น


Q&A