มติชน

ก6493

วันพุธที่ 14 กันยายน พุทธศักราช 2548 ปีที่ 28 ฉบับที่ 10049 หน้า 32

'Zero-Day' ความจริงของภัยคุกคามจากไฮเทค

มีนักวิจัยด้านความปลอดภัยของเทรนด์ ไมโคร พบการโจมตีแบบ "ซีโร่-เดย์" (Zero-Day) ที่ครั้งหนึ่งเคยคิดกันว่าเป็นแค่นิยายวิทยาศาสตร์นั้น เกิดขึ้นจริงแล้ว และได้รายงานเผยแพร่ไว้ในไมโครซอฟท์ ซีเคียวริตี้ บูลเลตติน ฉบับที่ MS05-038 เมื่อ 9 สิงหาคมที่ผ่านมา พร้อมกับประกาศขึ้นบนเว็บไซต์ยอดนิยม

นายเดวิด เพอร์รี ผู้อำนวยการฝ่ายการศึกษาและฝึกอบรมสำหรับบริษัทผู้ผลิตเนื้อหาเรื่องความปลอดภัยและการป้องกันไวรัสของเทรนด์ ไมโคร ซึ่งเคยเตือนเจ้าหน้าที่ด้านความปลอดภัยของทั้งภาครัฐและภาคเอกชนเมื่อ 2 ปีก่อน เกี่ยวกับระยะเวลาที่สั้นลงระหว่างการประกาศเตือนช่องโหว่และการค้นพบการใช้ประโยชน์ของช่องโหว่ หรือคอนเซปต์ของการใช้ประโยชน์จากช่องโหว่ "COM Object Instantiation Memory Corruption Vulnerability" (CAN-2005-1990) ของโปรแกรมอินเตอร์เน็ต เอ็กซ์พลอเรอร์ ว่าเมื่อปี 2543-2544 ผู้เขียนโปรแกรมไวรัสใช้เวลาหลังไมโครซอฟท์ออกประกาศความปลอดภัยฉบับที่ MS00-078 ประมาณ 11 เดือน พัฒนาไวรัสนิมดา ซึ่งใช้ช่องโหว่ในประกาศเตือนฉบับดังกล่าว

จากนั้นปี 2545 ช่วงห่างของระยะเวลาดังกล่าวลดลงเกือบครึ่งหนึ่ง โดยหลังประกาศเตือนฉบับที่ MS02-039 ก็ได้เห็นไวรัส SQLP ออกอาละวาดภายในเวลา 185 วัน ขณะที่อีก 6 เดือนต่อมา ไวรัส MSBLAST แพร่ระบาดไปทั่วเครือข่ายอินเตอร์เน็ตภายในระยะเวลาไม่ถึง 1 เดือน และเมื่อปีที่แล้ว เวิร์ม SASSER ใช้เวลาแค่ 17 วัน ในการเขียนโปรแกรมก่อนถูกส่งออกสร้างความเสียหายให้กับระบบคอมพิวเตอร์ทั่วโลก

เพอร์รีกล่าวว่า จากข้อมูลที่มีอยู่มากมาย ได้ตัดประสงค์ร้ายที่หาได้ตามเว็บไซต์อินเตอร์เน็ตสาธารณะทั่วไป รวมถึงระดับทักษะของผู้เขียนโปรแกรมมัลแวร์ที่เพิ่มสูงขึ้น เพอร์รีคาดว่าการโจมตีแบบซีโร่-เดย์ จะแพร่หลายมากขึ้นในอนาคตอันใกล้นี้

การใช้ประโยชน์จากช่องโหว่ทำงานได้อย่างไร และทำไมถึงอันตราย

เทรนด์ ไมโคร พิจารณาว่าการใช้ประโยชน์จากช่องโหว่เป็นอันตราย ไม่ใช่แค่เพราะผลกระทบที่เกิดขึ้น แต่รวมถึงความง่ายที่การโจมตีแต่ละครั้งจะเกิดขึ้นด้วย โดยครอบคลุมไปถึงการใช้เทคนิคการจัดการทางสังคมที่ประสบความสำเร็จไปแล้วหลายต่อหลายครั้ง การโจมตีที่ใช้จุดอ่อนในลักษณะนี้ไม่จำเป็นต้องใช้การปฏิสัมพันธ์จากผู้ใช้นอกเหนือไปจากการหลอกให้ผู้ใช้ให้เข้าไปในเว็บไซต์ปลอมซึ่งเป็นวิธีการโกงของฟิชชิ่งแบบเก่าที่ใช้แล้วประสบความสำเร็จเสมอ

โดยวิธีการทำงาน : แฮกเกอร์สร้างหน้าเว็บให้ใช้ประโยชน์จากช่องโหว่ได้ โดยสามารถสั่งให้โค้ดทำงานได้จากระยะไกลเมื่อผู้ใช้เปิดหน้าเว็บที่ว่านี้ จากนั้นแฮกเกอร์จะสั่งให้โค้ดทำงานได้จากระยะไกลในบริบทของผู้ใช้ที่ล็อกอินอยู่ ณ เวลานั้น หากผู้ใช้ล็อกอินด้วยสิทธิของ "ผู้ดูแลระบบ" แฮกเกอร์จะสามารถควบคุมคอมพิวเตอร์ของผู้ใช้ได้ทั้งหมด ติดตั้งโปรแกรมต่างๆ ประกอบด้วย สปายแวร์ ไวรัส และโปรแกรมประสงค์ร้ายอื่นๆ ได้ ทั้งสามารถดู เปลี่ยนลบข้อมูลหรือสร้างบัญชีใหม่ที่มาพร้อมกับสิทธิผู้ใช้เต็มรูปแบบ

แฮกเกอร์สามารถใช้เครื่องคอมพิวเตอร์ของผู้ใช้เป็น "ซอมบี้" เพื่อทำซ้ำไวรัส และโปรแกรมประสงค์ร้ายอื่นๆ รวมถึงช่วยให้โปรแกรมเหล่านี้แพร่ระบาดได้ง่ายขึ้น

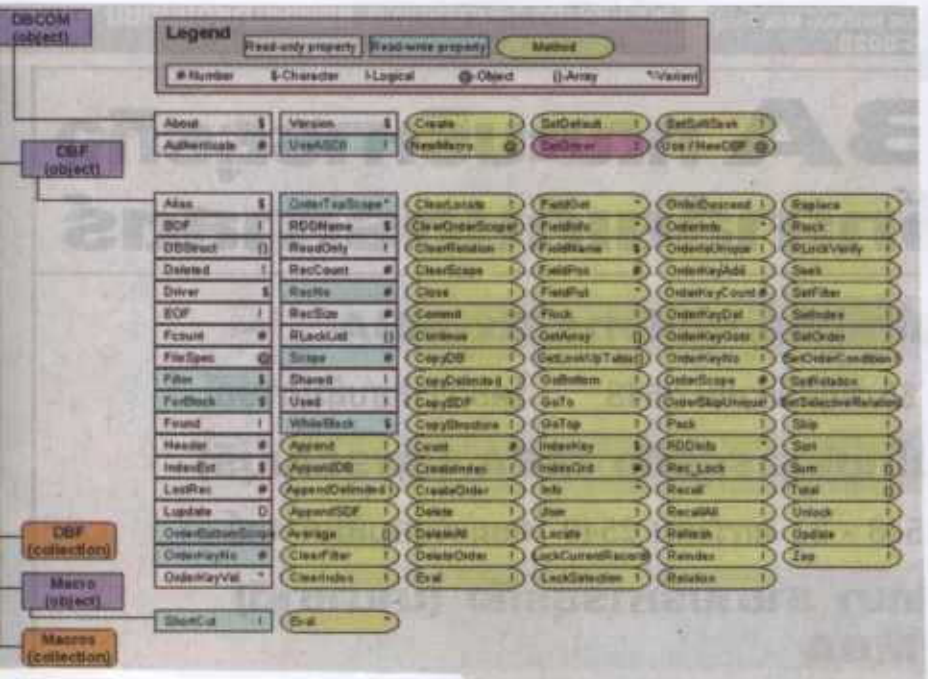
เพอร์รีอธิบายว่า การโจมตีแบบ "ซีโร่-เดย์" สามารถทำได้ง่ายภายใน 3 ขั้นตอนดังต่อไปนี้

1.โปรแกรมอินเตอร์เน็ต เอ็กซ์พลอเรอร์ มีช่องโหว่เปิดโอกาสให้ใช้ประโยชน์ได้ทาง COM Objects เมื่อโค้ดดังกล่าวถูกเขียนขึ้นเพื่อใช้ประโยชน์จาก Objects เหล่านี้ สิ่งที่นักเขียนโปรแกรมไวรัสต้องทำเพียงอย่างเดียว คือ ทดสอบกับ COM Objects เพื่อค้นหา Objects ตัวอื่นที่แสดงพฤติกรรมเหมือนกัน

2.ประกาศเรื่องความปลอดภัยของไมโครซอฟท์ ช่วยจัดหารายชื่อ "Vulnerable Objects" ฉบับสมบูรณ์ ซึ่งถูกสร้างขึ้นเพื่อแสดงพฤติกรรมที่คล้ายกับช่องโหว่ JVIEW Profiler โดยการอัพเดตจะกำหนดให้ทำลายเฉพาะ Objects ที่รู้จักแล้วเท่านั้น การสแกนรายชื่อดังกล่าว นักเขียนโปรแกรมไวรัสต้องการเพียงแค่ทดสอบ COM Objects ว่าเคยถูกตรวจพบไปแล้วหรือยัง เพื่อลดกระบวนการการทดสอบ

3.เมื่อทดสอบ COM object จนมั่นใจ นักเขียนโปรแกรมไวรัสสามารถเปลี่ยน CLSID ของไวรัสได้อย่าง

[ต่อหน้าหลัง]



ง่ายดาย และไวรัสสามารถใช้ Object ตัวอื่นได้

วิธีการใช้ประโยชน์จากช่องโหว่ในลักษณะนี้จะแพร่หลายมากขึ้น นักเขียนโปรแกรมไวรัสที่ฉลาดจะสามารถใช้ข้อมูลที่มีเป้าหมายเพื่อปกป้องผู้ใช้ไปในการสร้างความเสียหายให้กับผู้ใช้ได้อย่างง่ายดายและรวดเร็ว

ขณะที่ช่องโหว่จาก Web Folder Behaviors Cross-Domain (CAN-2005-1989) ช่องโหว่ข้ามโดเมนในโปรแกรมอินเตอร์เน็ต เอ็กซ์พลอเรอร์ สามารถถูกนำไปใช้ประโยชน์ในการเปิดเผยข้อมูลหรือสั่งให้โค้ดทำงานได้จากระยะไกลบนเครื่องที่ติดเชื้อได้ แฮกเกอร์อาจใช้ประโยชน์จากช่องโหว่นี้ด้วยการสร้างหน้าเว็บและส่ง ลวงให้ผู้ใช้เปิดดู โดยหน้าเว็บที่ว่านี้จะสั่งให้โค้ดทำงานได้จากระยะไกล นอกจากนี้ ยังสามารถควบคุมระบบ ของผู้ใช้ในขอบเขตของล็อคอินโพรไฟล์ของผู้ใช้ปัจจุบัน

ช่องโหว่ JPEG Image Rendering Memory Corruption(CAN-2005-1988) ช่องโหว่ที่สั่งให้โค้ดทำงานได้จากระยะไกลพบในโปรแกรมอินเตอร์เน็ต เอ็กซ์พลอเรอร์ เนื่องจากวิธีจัดการภาพเจเพ็ก การใช้ช่องโหว่นี้ แฮกเกอร์จะสร้างภาพเจเพ็กที่สามารถสั่งให้โค้ดทำงานบนเครื่องของผู้ใช้ได้จากระยะไกล ดังนั้น สิ่งเดียวที่แฮกเกอร์ต้องทำ คือ หลอกให้ผู้ใช้เปิดเว็บไซต์ที่บรรจุภาพเจเพ็กดังกล่าว หรือเปิดอ่านอี-เมลที่มีภาพเจเพ็กที่ว่านี้ฝังอยู่ในเนื้อความ และสิ่งที่แฮกเกอร์จะได้ คือ ควบคุมระบบของผู้ใช้ในขอบเขตของล็อคอิน โพรไฟล์ ของผู้ใช้ในปัจจุบัน

ผู้เชี่ยวชาญด้านความปลอดภัยเตือนว่า ช่องโหว่เหล่านี้เป็นอันตรายเนื่องจากเปิดช่องให้นักเขียนโปรแกรมไวรัสเข้าควบคุมเครื่องพีซีของผู้ใช้ได้เต็มรูปแบบ โดยในบางกรณีเพียงแค่ดูหน้าเว็บ หรืออี-เมลที่มีภาพเจเพ็กฝังอยู่เท่านั้น ตรงข้ามกับการโจมแบบฟิชชิง และไวรัสแบบเดิมที่ต้องอาศัยผู้ใช้ปฏิสัมพันธ์กับอี-เมลหรือเว็บไซต์ ซึ่งเป็นการเปิด "โอกาสครั้งที่สอง" ให้ผู้ใช้ได้คิดเกี่ยวกับการกระทำของตัวเองก่อนที่จะตกเป็นเหยื่อ

เจมส์ ยานเชา ผู้จัดการอาวุโสฝ่ายวิจัยป้องกันไวรัสของเทรนด์ ไมโคร บอกว่า ในบางครั้งการเปิดอี-เมลเฉยๆ ก็เพียงพอที่จะทำให้ถูกไวรัสโจมตีได้ สิ่งที่น่ากลัวที่สุดของช่องโหว่เหล่านี้ คือ ผู้ใช้ส่วนใหญ่ใช้ html ในอี-เมลของตัวเอง และโปรแกรมอี-เมลจำนวนมากก็ตั้งค่าเริ่มต้นให้เปิดอี-เมลทั้งหมดทันทีที่ถูกเลือก ทำให้ผู้ใช้ไม่สามารถเลือกข้อความที่จะลบทิ้งได้โดยไม่ติดเชื้อ

แม้จะมีเครื่องมือหลอกให้ผู้ใช้หลงเปิดดูเว็บไซต์ประสงค์ร้ายเหล่านี้มากมาย แต่นักวิจัยเชื่อว่า วิธีการธรรมดาที่ได้รับการพิสูจน์แล้วว่าใช้ได้ผล คือ อี-เมล และเทคนิคการจัดการทางสังคม เพื่อป้องกันตัวเองจากการโจมตีเหล่านี้มีคำแนะนำดังนี้

1.ตั้งค่าความปลอดภัยในโปรแกรมบราวเซอร์ให้สูงขึ้น ในกรณีที่แฮกเกอร์สามารถเจาะเข้ามาได้ในทุกระดับการตั้งค่าความปลอดภัยให้สูง จะทำให้โอกาสที่แฮกเกอร์จะหลุดเข้ามามีน้อยลง

2.จำกัดสิทธิผู้ใช้เมื่อออนไลน์ การใช้ช่องโหว่เหล่านี้แฮกเกอร์สามารถทำงานได้เฉพาะเมื่อมีสิทธิที่เหมือนกันกับผู้ใช้เท่านั้น ถ้าผู้ใช้ล็อคอินด้วยสิทธิผู้ใช้มาตรฐาน แฮกเกอร์อาจจะเข้าถึงได้ตามสิทธิของผู้ใช้มาตรฐานแต่ถ้าผู้ใช้ล็อคอินด้วยสิทธิของผู้ดูแลระบบ แฮกเกอร์ก็จะสามารถควบคุมพีซีของผู้ใช้ได้ทั้งหมด

3.เปลี่ยนค่ากำหนดรายละเอียดต่างๆของอี-เมลเป็น

a.ปิดคำสั่งโหลดอัตโนมัติเมื่อพรีวิวข้อความ

b.บล็อคภาพและเนื้อหาอินเตอร์เน็ตรูปแบบอื่นๆ รวมถึง html จากการดาวน์โหลดสู่เครื่องคอมพิวเตอร์โดยอัตโนมัติ

4.ฝึกพฤติกรรมการใช้อี-เมลโดยปลอดภัย ซึ่งรวมไปถึงการไม่คลิกลิงก์ที่ฝังอยู่ในอี-เมล

5.หลีกเลี่ยงการเปิดไฟล์แนบที่เป็นภาพ หรือไฟล์ประเภทอื่นๆ จากอี-เมลที่ส่งมาจากคนที่ไม่รู้จัก หรือแม้แต่คนที่รู้จัก แต่ไม่ได้ขอให้ส่งไฟล์มาให้

หากสงสัยให้ถามเจ้าของอี-เมลว่าส่งอะไรมาให้หรือเปล่า ก่อนที่จะเปิดไฟล์แนบใดๆ