เดลินิวส์
ฉบับที่ 20,962 วันจันทร์ที่ 5 มีนาคม พ.ศ. 2550 หน้า 12

ก 7445

ภัยคุกคามบนเว็บ

เงินที่ได้จากการจำหน่ายข้อมูลลับที่ขโมยมาถือเป็นสิ่งจูงใจของบรรดาเหล่ามิจฉาชีพไซเบอร์ และพวกเขากำลังจะใช้เว็บไซต์เป็นสื่อในการดำเนินการอันเลวร้ายด้วยการผสานเทคนิคที่มีอยู่ในปัจจุบัน ไม่ว่าจะเป็นการกระจายไวรัส และใช้การโจมตีอย่างมีเป้าหมาย จะเห็นได้ว่าภัยคุกคามบนเว็บสามารถก่อให้เกิดอันตรายได้อย่างครอบคลุม ทั้งการขโมยข้อมูลเฉพาะตัว การดึงข้อมูลขององค์กรที่เป็นความลับไปใช้งาน การทำให้ชื่อเสียงขององค์กรได้รับความเสียหาย และการดึงความลับของผู้ใช้งานอินเทอร์เน็ตทีละเล็กทีละน้อย

การขโมยข้อมูลลับเฉพาะ

ให้พิจารณาสถานการณ์สมมุติต่อไปนี้ โรเบิร์ต ทนายความในแผนกกฎหมายของบริษัทยายักษ์ใหญ่แห่งหนึ่ง ทุกวันที่เขามาถึงสำนักงาน สิ่งแรกคือการเข้าสู่ระบบคอมพิวเตอร์และตรวจดูอีเมลใหม่ที่ได้รับ โรเบิร์ตสังเกตเห็นว่ามีอีเมลฉบับหนึ่งที่มีลิงก์ไปยังเว็บไซต์ใหม่ที่มีข้อมูลเกี่ยวกับนักเบสบอลทีมโปรดของเขา และในฐานะที่เป็นแฟนเบสบอลตัวยง โรเบิร์ตจึงคลิกลิงก์ดังกล่าว ซึ่งได้พาเขาไปยังเว็บไซต์แห่งหนึ่งที่มีรูปภาพ วิดีโอ และเนื้อหาต่าง ๆ ของนักกีฬาที่เขาชื่นชอบ แต่ด้วยความรู้เท่าไม่ถึงการณ์ของโรเบิร์ต ทันทีที่เบราเซอร์ของเขาแสดงรูปภาพหนึ่งขึ้นมา โค้ดร้ายที่มีแฝงอยู่ในไฟล์สกุล jpg ก็จะสั่งการให้คอมพิวเตอร์ของเขาดาวน์โหลดไฟล์ปฏิบัติการ (.exe) ซึ่งจะถูกดำเนินการโดยอัตโนมัติ จากนั้นมัลแวร์ตัวนี้จะเข้าไปดึงไฟล์ที่ต้องการในฮาร์ดดิสก์ของโรเบิร์ต จัดการบีบอัดและเข้ารหัสไฟล์เหล่านั้น แล้วส่งต่อไปยังที่อยู่อีเมลบุคคลที่สาม ซึ่งก็คือที่อยู่ของเหล่ามิจฉาชีพไซเบอร์นั่นเอง ไฟล์เหล่านี้บางไฟล์เป็นข้อมูลลับเกี่ยวกับคดีด้านสิทธิบัตรหลายคดีที่โรเบิร์ตรับผิดชอบอยู่ และวิธีการเดียวกันนี้ก็ยังถูกนำไปใช้กับพนักงานของบริษัทยาอื่น ๆ ด้วย โดยเหล่ามิจฉาชีพไซเบอร์มีเป้าหมายไปที่อุตสาหกรรมยาเพื่อให้ได้ข้อมูลลักษณะดังกล่าวและนำไปขายต่อเพื่อสร้างรายได้ให้กับตัวเอง

การคลิกลิงก์เพื่อไปยังเว็บไซต์เบสบอลที่ดูเหมือนว่าจะไม่เป็นของโรเบิร์ต ได้สร้างกระบวนการที่ทำให้ข้อมูลลับขององค์กรตกอยู่ในมือของวายร้ายโดยไม่ตั้งใจ การกระทำครั้งนี้ได้ส่งผลให้บริษัทของเขาจะสูญเสียข้อมูลด้านคดีความสิทธิบัตร เกิดความยุ่งเหยิงทางด้านกฎหมาย และมีค่าเสียหายอื่น ๆ ตามมา

ในเช้าวันเดียวกันนั้น ผู้ดูแลระบบไอทีของบริษัทยาแห่งนี้กำลังตรวจสอบการจราจรของเครือข่าย และด้วยความมั่นใจในระบบป้องกันไวรัสที่ใช้การกรองรายชื่อของยูอาร์แอล (URL) ผู้ดูแลระบบจึงไม่เห็นกิจกรรมที่ผิดปกติบนหน้าจอ แต่จริง ๆ แล้วผู้เขียนมัลแวร์สามารถหลีกเลี่ยงการตรวจจับดังกล่าวได้ด้วยการสร้างเว็บไซต์ใหม่ที่มีเนื้อหาร้ายแฝงอยู่ ดังนั้นยูอาร์แอลใหม่ ๆ นี้จึงยังไม่ถูกรวมอยู่ในรายชื่อเว็บไซต์ที่ซอฟต์แวร์กรองยูอาร์แอลมี มิจฉาชีพไซเบอร์มักจะใช้คำสั่งที่สั่งการให้มัลแวร์เพื่อค่อย ๆ ส่งออกไฟล์ของโรเบิร์ตมาภายนอก เพื่อหลีกเลี่ยงไม่ให้กระทบต่อการจราจรของเครือข่ายที่ผู้ดูแลระบบอาจสังเกตเห็นได้ และเนื่องจากบริษัทยาแห่งนี้ยังไม่ได้ติดตั้งซอฟต์แวร์ป้องกันใด ๆ ไว้ที่เกตเวย์เพื่อวิเคราะห์พฤติกรรมดังกล่าว จึงยากที่จะรู้ถึงความผิดปกติในคอมพิวเตอร์ของโรเบิร์ตเครื่องมือวัดความปลอดภัยขั้นสูงเป็นสิ่งจำเป็น

โชคไม่ดีที่ทั่วโลกสามารถเกิดสถานการณ์สมมุติเช่นเดียวกันนี้ได้ และสิ่งนี้กำลังเกิดขึ้นในองค์กรขนาดใหญ่และรวมถึงธุรกิจขนาดเล็กด้วยหรือแม้แต่ตัวผู้บริโภคเองก็มีสิทธิจะโดนขโมยข้อมูลลับได้เช่นกัน

"ภัยคุกคามบนเว็บ" กำลังเติบโตและเพิ่มจำนวนมากขึ้นดังตัวอย่างที่กล่าวมาข้างต้น โดยเป้าหมายที่มิจฉาชีพไซเบอร์ต้องการมีหลายอย่าง อาทิ หมายเลขประกันสังคมจากองค์กรด้านดูแลสุขภาพ หมายเลขบัตรเครดิตจากสถาบันการเงิน ข้อมูลเฉพาะตัวจากบริษัทด้านเทคโนโลยี

นอกจากจะสามารถขโมยข้อมูลลับไปได้โดยง่ายแล้ว วิธีการดังกล่าวยังเป็นการทำลายสิทธิส่วนบุคคลของผู้บริโภค ทำลายระบบธนาคารออนไลน์ การทำธุรกรรมและอีคอมเมิร์ซผ่านทางอินเทอร์เน็ตทีละน้อย ระบบป้องกันเดิมที่มีอยู่ดูเหมือนว่าจะไม่สามารถสร้างแนวป้องกันภัยคุกคามเหล่านี้ได้อย่างเพียงพอ และไม่มีวิธีการหรือเทคโนโลยีเดียวที่จะแก้ไขสถานการณ์นี้ให้ดีขึ้นได้ ต้องใช้เทคนิคการป้องกันขั้นสูงและหลายชั้น โดยแต่ละเทคนิคต้องถูกนำมารวมเข้าด้วยกันเพื่อให้เกิดความสมบูรณ์.