เทรนด์ไมโครเตือนองค์กรธุรกิจระวังถูกล้วงข้อมูลสำคัญ หลังอาชญากรไซเบอร์เลือกใช้การโจมตีแบบมีเป้าหมายเพิ่มขึ้น

นายแม็คกี้ ครูซ ฝ่ายการสื่อสารด้านเทคนิค ศูนย์วิจัยเทรนด์แล็บส์ บริษัท เทรนด์ไมโคร อิงค์ เปิดเผยว่า “การจารกรรมข้อมูลคือการที่ข้อมูลสำคัญถูกถ่ายโอนโดยไม่ได้รับอนุญาตจากเครือข่ายเป้าหมายไปยังตำแหน่งที่ตั้งที่ควบคุมโดยผู้ก่อการร้าย และเนื่องจากข้อมูลบนเครือข่ายขององค์กรมักจะมีการย้ายเข้าและออกเป็นประจำ ดังนั้น การจารกรรมข้อมูลจึงดูเหมือนกับการรับส่งข้อมูลปกติบนเครือข่าย ซึ่งนั่นทำให้การตรวจจับการจารกรรมดังกล่าวสร้างปัญหาให้กับกลุ่มผู้ดูแลความปลอดภัยสำหรับระบบไอทีได้”

ข้อมูลที่ไหลเข้าก่อให้เกิดค่าใช้จ่าย การจารกรรมข้อมูลทางไซเบอร์ก่อให้เกิดค่าใช้จ่ายอย่างเห็นได้ชัด ซึ่งระบบคำนวณความเสี่ยงจะเริ่มพิจารณาค่าใช้จ่ายตั้งแต่ระยะแรกที่มีการตรวจพบการละเมิด ได้แก่ กิจกรรมที่ตอบสนองต่อเหตุการณ์ที่เกิดขึ้น การจัดการภาวะวิกฤต และบทลงโทษที่เกี่ยวข้องกับการไม่ปฏิบัติตามกฎระเบียบ การสูญเสียความได้เปรียบในการแข่งขันจากการที่ข้อมูลซึ่งเป็นทรัพย์สินทางปัญญาขององค์กรถูกนำไปขายให้กับบริษัทคู่แข่งสามารถคุกคามความอยู่รอดขององค์กรธุรกิจได้อย่างมาก โดยคำว่า “สูญเสีย” ไม่เพียงหมายถึงค่าใช้จ่ายจากการวิจัยและพัฒนาในการปรับปรุงผลิตภัณฑ์เท่านั้น แต่ยังรวมถึงการสูญเสียโอกาสด้านการขายและการเป็นผู้นำในตลาดด้วย ตัวอย่างเช่น การโจมตีที่เรียกว่า **เครือข่ายเงา (Shadow Network)** ช่วยให้ผู้โจมตีสามารถโยกย้ายเอกสารในหมวดหมู่ความลับ (Secret), ลับเฉพาะ (Confidential) และปกปิด (Restricted) และเมื่อมีการเผยแพร่เอกสารที่ถูกแท็กไว้ในหมวดหมู่ดังกล่าวออกสู่สาธารณะก็อาจเป็นอันตรายต่อความมั่นคงของชาติได้ เช่น เอกสารปกปิดที่เป็นข้อมูลเกี่ยวกับการออกแบบ การสร้าง และการใช้วัสดุหรืออาวุธนิวเคลียร์ เป็นต้น

แม้ว่าการโจมตีแบบมีเป้าหมายจะเห็นผลได้อย่างชัดเจนอยู่แล้ว แต่ก็ดูเหมือนว่าความพยายามในการยักย้ายถ่ายโอนข้อมูลจากภายในเครือข่ายที่ถูกแทรกซึมก็กำลังเพิ่มจำนวนมากขึ้นเรื่อยๆ เมื่อเร็วๆ นี้ เทรนด์ไมโครได้เผยแพร่รายงานเกี่ยวกับแคมเปญของการโจมตีแบบมีเป้าหมายที่ใช้ **EvilGrab** โดยที่ผู้ก่อการร้ายจะเริ่มต้นด้วยการเข้าไปยังประตูหลังของระบบที่สามารถบันทึกการกดแป้นพิมพ์ รวมถึงวิดีโอและเสียงของสภาพ

แวดล้อมการทำงานของระบบโดยใช้ไมโครโฟนและกล้องวิดีโอที่เชื่อมต่ออยู่กับระบบ คุณลักษณะเหล่านี้เอื้อต่อการทำงานของโทรจันเชื่อมต่อจากระยะไกล และเหมือนกับการลักลอบขโมยข้อมูลทั่วไป นั่นคือข้อมูลที่ถูกขโมยดังกล่าวจะถูกอัพโหลดไปยังเซิร์ฟเวอร์ระยะไกลที่ผู้โจมตีสามารถเข้าถึงได้โดยใช้ความสามารถด้านการถ่ายโอนไฟล์ที่มีอยู่ในตัวของโทรจันเชื่อมต่อจากระยะไกล

ทั้งนี้ โทรจันเชื่อมต่อจากระยะไกลเป็นมัลแวร์ที่ช่วยให้อาชญากรไซเบอร์สามารถเข้าควบคุมระบบที่ถูกบุกรุกได้อย่างเต็มรูปแบบ โดยโทรจันเชื่อมต่อจากระยะไกลหรือเครื่องมือโจมตีอื่นๆ ที่มีคุณสมบัติเหมือนกันมักจะถูกนำมาใช้งานเสมอ เนื่องจากในขั้นตอนแรกเริ่มของการโจมตีแบบมีเป้าหมายนั้น จะต้องใช้การสื่อสารและการควบคุมแบบเรียลไทม์โดยผู้โจมตีระบบดังกล่าว

นอกจากนี้ อาชญากรไซเบอร์ยังสามารถใช้คุณลักษณะที่มีอยู่ในวินโดว์สให้เป็นประโยชน์ได้เช่นกัน โดยอาจใช้ WMI (Windows Management Instrumentation) เพื่อติดตามตรวจสอบและบันทึกไฟล์ที่มีการเปิดล่าสุด และสามารถใช้ FTP หรือ HTTP ในการส่งไฟล์เพื่อหลอกให้ผู้ดูแลระบบไอทีเข้าใจว่าการรับส่งข้อมูลบนเครือข่ายดังกล่าวเป็นการสื่อสารที่เป็นปกติ

นักวิจัยของเทรนด์ไมโครคาดการณ์ว่า ในอนาคตผู้ก่อการร้ายจะไม่เพียงแต่พุ่งเป้าไปที่การขโมยข้อมูลเท่านั้น แต่จะทำการปรับเปลี่ยนแก้ไขข้อมูลด้วย ซึ่งนั่นจะเปลี่ยนโฉมของการโจมตีแบบมีเป้าหมายจากการ จารกรรมข้อมูลไปเป็นการก่อวินาศกรรมได้

บริษัท เทรนด์ไมโครแนะนำแนวทางปฏิบัติเพื่อให้องค์กรพร้อมรับมือกับภัยคุกคามต่างๆ ดังนี้ องค์กรธุรกิจควรห้ามให้สิทธิ์ระดับผู้ดูแลระบบแก่ผู้ใช้ทั่วไป และควรปิดช่องโหว่ในระบบตั้งแต่แรกเริ่ม รวมทั้งเตรียมวางแผนและทีมงานเพื่อตอบสนองต่อเหตุการณ์โดยเฉพาะและรวมศูนย์การติดตามตรวจสอบเหตุการณ์และบันทึกเกี่ยวกับความปลอดภัย

อีกทั้งควรตรวจหาและบล็อกการโจมตีฟิชชิ่งแบบเจาะจงเป้าหมายที่ระดับแนวป้องกัน และเพิ่มความสามารถในการมองเห็นการสื่อสารแบบ C&C บนเครือข่าย และด้านการป้องกันช่องโหว่ต่อระบบที่สำคัญ รวมทั้งปรับใช้ความสามารถด้านระบบ Sandbox ที่สามารถปรับแต่งได้เพื่อวิเคราะห์มัลแวร์ที่ออกแบบมาโจมตีในช่วงซีโร่เดย์โดยเฉพาะและควรติดตามตรวจสอบระบบที่สำคัญเพื่อค้นหาการเปลี่ยนแปลงที่ไม่ได้รับอนุญาตด้วยการตรวจสอบความสมบูรณ์ของไฟล์ด้วย

สำหรับรายละเอียดเกี่ยวกับชนิดของเครื่องมือและเทคนิคที่อาชญากรไซเบอร์ใช้ในแคมเปญการโจมตีแบบมีเป้าหมาย คลิกดูได้ที่ **http://about-threats.trendmicro.com/cloud-content/us/entprimers/pdf/how_do_threat_actors_steal_your_ data.pdf**