เทรนด์ ไมโคร เตือนระวังอาชญากรไซเบอร์ใช้ข้อความสแปมโอลิมปิก ลอนดอน 2012 เพื่อล้วงข้อมูลส่วนตัวและขโมยเงิน

รายงานล่าสุดจากศูนย์วิจัยเทรนด์แล็บส์ บริษัท เทรนด์ ไมโคร อิงค์ เปิดเผยว่า อาชญากรไซเบอร์ได้ชื่อว่าเป็นนักฉวยโอกาสตัวยงที่มักจะใช้ประโยชน์จากเหตุการณ์ต่างๆ ที่อยู่ในกระแส เช่น ในช่วงมหกรรมการแข่งขันกีฬาครั้งสำคัญ เช่น FIFA หรือโอลิมปิก และได้นำเหตุการณ์เหล่านั้นมาสร้างเป็นแผนการเฉพาะของตนขึ้นมา แน่นอนว่ามหกรรมโอลิมปิก ลอนดอน 2012 ซึ่งกำลังจะมีขึ้นในเร็วๆ นี้ ข้อความสแปมที่ใช้ประโยชน์จากเหตุการณ์ดังกล่าวจะมีจำนวนเพิ่มขึ้นอย่างมากเช่นกัน

ต่อไปนี้คือข้อความสแปมบางอย่างที่เราพบว่ามีการใช้เหตุการณ์โอลิมปิก 2012 เป็นเหยื่อล่อ โดยข้อความหนึ่งในนั้นจะเกี่ยวข้องกับอีเมล “การแจ้งผลรางวัล” (winning notification) ขณะที่อีกข้อความจะขอให้ผู้ใช้ระบุรายละเอียดส่วนตัวเพื่อแลกกับของรางวัล และอีกฉบับจะขอให้ผู้ใช้ติดต่อกลับไปยังบุคคลที่ระบุชื่อไว้ในอีเมล ผู้ใช้ที่ตกหลุมพรางดังกล่าวอาจเสี่ยงที่ข้อมูลจะถูกขโมยหรืออาจทำให้เครื่องคอมพิวเตอร์ของตนติดมัลแวร์ได้ นอกจากนี้ สแปมบางอย่างยังอาจนำไปสู่การสูญเสียในรูปของตัวเงินได้อีกด้วย

รางวัลตั๋วฟรีแลกกับข้อมูลของคุณ สแปมที่เกี่ยวข้องกับโอลิมปิกที่เราตรวจพบชนิดแรกคืออีเมลที่ขอให้ผู้ใช้ระบุข้อมูลส่วนตัว โดยผู้ใช้มักจะเต็มใจมอบรายละเอียดดังกล่าวให้ เนื่องจากข้อความที่พวกเขาได้รับเป็นการแจ้งว่าพวกเขาได้รับรางวัลเป็นตั๋วฟรี และเพื่อรับสิทธิ์ในรางวัลดังกล่าว ผู้ใช้จะต้องเปิดเผยข้อมูลส่วนตัว เช่น ที่อยู่ สถานภาพสมรส และอาชีพ นอกจากนี้ ข้อความดังกล่าวยังอาจจะล่อลวงหนักขึ้นด้วยการแจ้งเหยื่อว่าได้รับรางวัลใหญ่เป็นเงินสดอีกด้วย ผู้ล่อลวงที่อยู่เบื้องหลังสแปมดังกล่าวอาจใช้ข้อมูลที่เก็บรวบรวมได้สำหรับแผนการร้ายในภายหลัง และยังอาจนำข้อมูลดังกล่าวไปขายให้กับกลุ่มอาชญากรอื่นๆ ด้วย

มัลแวร์ลวงในรูปการแจ้งผลรางวัล

นอกจากนี้ เรายังพบข้อความสแปมหลายอย่างเกี่ยวกับโอลิมปิก ลอนดอน 2012 ที่มาในรูปของไฟล์แนบที่ระบุว่าเป็น “การแจ้งผลรางวัล” (winning notifications) และมีรายละเอียดเกี่ยวกับรางวัลอยู่ในไฟล์ดังกล่าว ผู้ใช้ที่อยากรู้และได้ทำการดาวน์โหลดและเปิดไฟล์แนบนั้น ก็จะเป็นการเรียกใช้ไฟล์ปฏิบัติการที่เป็นอันตรายในทันที

สำหรับการทำงานของสแปมอื่นๆ เราพบข้อความที่มีไฟล์แนบที่จริงๆ แล้วเป็นโทรจัน (ตรวจพบว่าเป็น TROJ_ARTIEF.ZIGS) ซึ่งจะใช้ประโยชน์จากช่องโหว่ RTF Stack Buffer Overflow Vulnerability (CVE-2010-3333) โดยเมื่อช่องโหว่สัมฤทธิ์ผล มัลแวร์จะทิ้ง BKDR_CYSXL.A ไว้ทางประตูหลังของระบบ จากการวิเคราะห์ของเรา ประตูหลังดังกล่าวจะเชื่อมต่อกับผู้ใช้ระยะไกลที่อาจเรียกใช้คำสั่งบนระบบที่ติดเชื้อ แต่สิ่งที่น่าเป็นกังวลอย่างมากก็คือประตูหลังของระบบที่เปิดอยู่นั้นจะเป็นการเปิดช่องให้เกิดภัยคุกคามอื่นๆ ตามมาด้วย ซึ่งอาจรวมถึงมัลแวร์ขโมยข้อมูลประจำตัวสำหรับการทำธุรกรรมธนาคารออนไลน์ (รหัสผ่าน ชื่อผู้ใช้ เป็นต้น)

สแปมที่ขอให้ผู้ใช้ติดต่อบุคคลที่เฉพาะเจาะจง สแปมชนิดที่สามารถดู

เหมือนว่าเป็นข้อความปกติในครั้งแรก แต่เมื่อตรวจสอบแล้ว กลับพบว่าข้อความนั้นอาจอ้างว่ามาจากองค์กรที่เป็นที่รู้จักกันดี เช่น Visa และมีรายละเอียดที่ติดต่อของผู้ประสานงานหรือบุคคลติดต่อสำหรับโปรโมชั่นลวงนั้นๆ ในข้อความที่ได้รับจะมีการแนะนำให้ผู้รับติดต่อกลับไปยัง “ผู้ประสานงาน” ที่สมมติขึ้นซึ่งมีชื่อระบุไว้ในข้อความ เมื่อผู้ใช้ตอบกลับที่อยู่ดังกล่าว พวกเขาก็จะได้รับการตอบกลับจากผู้หลอกลวงพร้อมด้วยคำแนะนำเกี่ยวกับวิธีการขอรับรางวัล และในท้ายที่สุดผู้ใช้ก็จะถูกขอให้ระบุข้อมูลส่วนตัว นอกจากนี้ผู้อยู่เบื้องหลังภัยคุกคามนี้อาจขอให้ผู้ใช้ระบุรายละเอียดบัญชีหรือโอนเงินไปยังบัญชีธนาคารเฉพาะเพื่อแลกกับรางวัลที่พวกเขาจะได้รับก็ได้

เหตุใดแสปมรูปแบบเหล่านี้จึงยังคงอยู่ การหลอกลวงในลักษณะดังกล่าวไม่ใช่สิ่งใหม่ อย่างสแปมที่เกิดขึ้นในช่วงก่อนหน้านี้เป็นการใช้ประโยชน์จากโอลิมปิก ปักกิ่ง 2008 (Beijing Olympics 2008) และการแข่งขันกีฬาโอลิมปิกฤดูหนาว ณ เมืองโตริโน่ (Torino Winter Games) การที่กลลวงเหล่านี้ยังคงมีอยู่ก็เนื่องมาจากอาชญากรไซเบอร์ยังคงทำเงินได้จากภัยคุกคามในลักษณะนี้ **โรเบิร์ต แมคอาร์เดล นักวิจัยอาวุโสด้านภัยคุกคาม ศูนย์วิจัยเทรนด์แล็บส์ เชื่อว่า** *“...ผู้โจมตีจะยังคงใช้กลลวงรูปแบบดังกล่าวอยู่ เนื่องจากสามารถสร้างประโยชน์ให้กับพวกเขาได้อย่างต่อเนื่อง จะเห็นได้ว่าแม้เทคนิควิศวกรรมทางสังคมจะถูกใช้มาเป็นเวลาหลายปีแล้วแต่กลับมีแนวโน้มที่จะเกิดการเปลี่ยนแปลงน้อยมาก”* ดังนั้น ตราบเท่าที่ผู้ใช้ยังคงตกหลุมพรางนี้อยู่ ผู้หลอกลวงก็จะยังคงสร้างสแปมใหม่ๆ ที่อาศัยเหตุการณ์ในกระแส เช่น โอลิมปิก ลอนดอน เพื่อล่อลวงเหยื่ออยู่ดี บริษัทเทรนด์ ไมโคร ปกป้องผู้ใช้จากภัยคุกคามนี้ผ่านทางสมาร์ท โพรเทคชั่น เน็ตเวิร์ค (Smart Protection Network™) ซึ่งมีบริการตรวจสอบประวัติเว็บที่จะทำหน้าที่บล็อกข้อความสแปมในลักษณะดัง กล่าวไม่ให้เข้าถึงกล่องจดหมายของผู้ใช้ ขณะที่บริการตรวจสอบประวัติไฟล์จะช่วยตรวจหาและลบมัลแวร์ที่เกี่ยวข้องออกไปให้ด้วย นอกจากนี้ผู้ใช้ยังสามารถป้องกันภัยคุกคามเหล่านี้ได้ด้วยการตรวจสอบอีเมลด้วยตัวเองแบบง่ายๆ โดยอีเมลที่ไม่ปกติจะมีสัญญาณบ่งบอกบางอย่างที่เห็นได้อย่างชัดเจน ได้แก่

- มีรูปแบบอีเมลไม่เป็นระเบียบหรือไม่ใช่แบบมืออาชีพ
- ข้อความที่ใช้เขียนผิดไวยากรณ์อย่างเห็นได้ชัด

- อ้างถึงเงินรางวัลที่มีจำนวนมากอย่างไม่น่าเชื่อ

ข้อมูลโดย เมดาลีน ซัลวาดอร์ วิศวกรด้านการวิจัยระบบป้องกันสแปม ศูนย์วิจัยเทรนด์แล็บส์