เทรนด์ไมโครเตือนระวังภัยอีเมลฟิชชิ่งหลอกลวงผู้ใช้อินเทอร์เน็ต

บริษัท เทรนด์ไมโคร อินคอร์ปอเรท (TYO: 4704; TSE: 4704) ผู้นำระดับโลกด้านการรักษาความปลอดภัยสำหรับระบบคลาวด์เปิดเผยว่าล่าสุดตรวจพบการโจมตีที่ใช้ประโยชน์จากความสนใจของทั่วโลกที่มีต่อพิธีสาบานพระองค์รับตำแหน่งประมุขแห่งคริสตจักรนิกายโรมันคาทอลิกของสมเด็จพระสันตะปาปา ฟรานซิสด้วยการส่งสแปมที่มีลิงก์ข่าวปลอมฝังอยู่ภายในโดยอีเมลอันตรายดังกล่าวมีลักษณะเหมือนกับการแจ้งข่าวสารจริงจากเว็บไซต์ข่าวที่เป็นทางการ และลิงก์ลวงดังกล่าวก็จะนำเหยื่อที่หลงเชื่อไปสู่มัลแวร์อันตรายในท้ายที่สุด

นายพอล โอลิเวอร์เรีย หัวหน้าฝ่ายซีเคียวริตี้โฟกัสจากศูนย์วิจัยเทรนด์แล็บส์ บริษัท เทรนด์ไมโคร กล่าวว่า “บริษัทเทรนด์ไมโครพบว่าสแปมข่าวจะล่อลวงให้ผู้ใช้งานอินเทอร์เน็ตคลิกลิงก์ในอีเมล โดยใช้พาดหัวที่เกี่ยวข้องกับสมเด็จพระสันตะปาปาฟรานซิสและข้อโต้แย้งเกี่ยวกับนิกายคาทอลิก เนื้อหาของอีเมลฟิชชิ่งเหล่านี้จะดูเหมือนกับข้อความปกติส่วนใหญ่ เช่น การรายงานข่าวจากสำนักข่าวซีเอ็นเอ็น จากนั้นลิงก์ที่ฝังอยู่ในสแปมเหล่านี้จะนำเหยื่อที่หลงเชื่อเข้าไปยังเว็บไซต์ที่ได้รับการสนับสนุนจาก Blackhole Exploit Kit (BHEK) ซึ่งเป็นเครื่องมือที่เปิดช่องให้มัลแวร์อันตรายเข้าโจมตี การทำงานของสแปม BHEK จะเกิดขึ้นในทันทีและดำเนินการอย่างต่อเนื่องเพื่อให้เกิดผลลัพธ์ในระดับสูง ผู้ใช้งานอินเทอร์เน็ตควรระมัดระวังเมื่อได้รับอีเมลที่มีลิงก์ เพื่อป้องกันอันตรายจากมัลแวร์และฟิชชิ่งที่แฝงมาด้วย”

BHEK จะเปิดช่องให้กับมัลแวร์ เช่น ตัวขโมยข้อมูล แบ็คดอร์ รีโมท แอคเซส โทรจัน และรูทคิตส์ ส่งผลให้ผู้ใช้งานตกอยู่ในอันตรายจากการถูกขโมยข้อมูลหรือทำให้อุปกรณ์ของตนเชื่อมต่อเข้ากับเครือข่ายบ็อตเน็ตโดยไม่รู้ตัว

นายพอลกล่าวเพิ่มเติมว่า “ไม่ว่าคุณจะเป็นชาวคาทอลิกหรือไม่ก็ตาม การประกาศสละสมณศักดิ์ของสมเด็จพระสันตะปาปาเบเนดิกต์ และพิธีสาบานพระองค์ของสมเด็จพระสันตะปาปาองค์ใหม่ ถือเป็นข่าวที่ทุกคนให้ความสนใจอย่างมาก โดยอาชญากรไซเบอร์มักจะใช้โอกาสนี้หลอกลวงผู้ใช้งานอินเทอร์เน็ตและประชาชนที่ต้องการทราบข่าวสารดังกล่าว ดังนั้นผู้ใช้งานอินเทอร์เน็ตจึงต้องเพิ่มการป้องกันให้มากขึ้นด้วย”

และเพื่อช่วยให้ผู้ใช้ปลอดภัยจากการโจมตีเหล่านี้ได้ บริษัทเทรนด์ไมโครจึงพัฒนาเทคโนโลยีใหม่ซึ่งใช้ประโยชน์จากเครือข่ายป้องกันภัยอัจฉริยะ (สมาร์ท โพรเท็คชั่น เน็ตเวิร์ก) ที่มีคุณสมบัติเด่นๆ ดังนี้

• **ตรวจจับข้อความฟิชชิ่งด้วยการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data)** – โซลูชั่นเชิงรุกนี้จะใช้ขีดความสามารถที่หลากหลายและจะแสดงให้เห็นภาพของการเชื่อมโยงที่เป็นเครือข่ายของกลุ่มและชุมชนต่างๆ โดยข้อมูล

เช่น เทมเพลตอีเมล, ที่อยู่ IP และส่วนประกอบอื่นๆ จะเป็นสิ่งสำคัญที่ใช้ในการเชื่อมโยงความสัมพันธ์และพฤติกรรมภายในเครือข่ายนั้นๆ

• **เปรียบเทียบพฤติกรรมของข้อความกับระบบอัจฉริยะที่โซลูชั่นนี้พัฒนาขึ้น –** โซลูชั่นนี้จะระบุว่าข้อความเป็นฟิชชิ่งหรืออีเมลอันตรายหรือไม่ จากการพิจารณาพฤติกรรมและส่วนประกอบของข้อความนั้นๆ

• **ระบุการโจมตีเหล่านี้เมื่อเพจที่เป็นฟิชชิ่งเริ่มดำเนินการหรือมีการเปลี่ยนแปลง –** ความ สามารถที่เพิ่มขึ้นในการตรวจจับการโจมตีฟิชชิ่งด้วยระยะเวลาที่สั้นที่สุด โดยขณะนี้เครือข่ายป้องกันภัยอัจฉริยะ (สมาร์ท โพรเท็คชั่น เน็ตเวิร์ก) สามารถตรวจจับและบล็อกข้อความสแปมและ URL ที่เกี่ยวข้องทั้งหมดไว้แล้ว

สำหรับข้อมูลเพิ่มเติมโปรดคลิกดูได้ที่:
http://cloudsecurity.trendmicro.com/us/technology-innovation/our-technology/smart-protection-network/index.html