เทรนด์ไมโครเตือนระวังมัลแวร์บนเฟซบุ๊กช่วงวาเลนไทน์

นายคริสโตเฟอร์ ทาแลมปัส นักวิเคราะห์จากศูนย์วิจัยเทรนด์แล็บส์ บริษัท เทรนด์ไมโคร เปิดเผยว่า “เมื่อเร็ว ๆ นี้ เราได้พบการหลอกลวงในเฟซบุ๊กที่เริ่มใช้ประโยชน์จากเทศกาลแห่งความรักที่กำลังจะมาถึงนี้ การโจมตีดังกล่าวเริ่มต้นด้วยการโพสต์บนวอลล์ของผู้ใช้เพื่อเชิญให้ผู้ใช้คนอื่นๆ ติดตั้งธีมวาเลนไทน์ลงในโปรไฟล์เฟซบุ๊กของตน”

เมื่อผู้ใช้คลิกที่โพสต์นี้ ระบบก็จะนำพวกเขาไปยังอีกเพจที่แจ้งให้พวกเขาดำเนินการติดตั้งธีมดังกล่าว โดยการโจมตีนี้จะทำงานเฉพาะในเบราว์เซอร์ *Google Chrome* หรือ *Mozilla Firefox* เท่านั้น

การคลิกปุ่ม *Installl (ติดตั้ง)* บนเพจดังกล่าวจะนำไปสู่การดาวน์โหลดไฟล์ที่เป็นอันตรายที่ชื่อว่า FacebookChrome.crx ซึ่งบริษัทเทรนด์ไมโคร ตรวจพบว่าเป็น **TROJ_FOOKBACE.A** และเมื่อเรียกใช้ไฟล์ที่ดาวน์โหลดมาแล้ว TROJ_FOOKBACE.A ก็จะดำเนินการรันสคริปต์ที่มีความสามารถในการแสดงโฆษณาจากเว็บไซต์บางแห่ง นอกจากนี้ มัลแวร์ดังกล่าวยังจะติดตั้งตัวเองในเบราเซอร์ของผู้ใช้ในรูปของส่วนขยายที่ชื่อว่า *Facebook Improvement |Facebook.com* ด้วย

เมื่อส่วนขยายเบราว์เซอร์ที่เป็นอันตรายนี้ได้รับการติดตั้ง ก็จะทำการติดตามกิจกรรมการท่องเว็บของผู้ใช้ และเปลี่ยนเพจของผู้ใช้ไปยังเพจการสำรวจเพื่อขอให้ผู้ใช้ระบุหมายเลขโทรศัพท์มือถือของตน สำหรับผู้ใช้ที่คลิกโพสต์ดังกล่าวผ่านทางเบราว์เซอร์ Internet Explorer (IE) ระบบจะนำผู้ใช้ไปยังเพจแบบสำรวจเช่นเดียวกันแต่จะไม่มีการขอให้ดาวน์โหลดสิ่งใด

เมื่อทำการวิเคราะห์เพิ่มเติม เราพบว่าการโจมตีนี้จะมีประสิทธิภาพมากขึ้นหากผู้ใช้กำลังใช้งานเบราว์เซอร์ *Google Chrome* หรือ *Mozilla Firefox* อยู่ เนื่องจากจะมีลักษณะเหมือนกับการดาวน์โหลดส่วนขยายเบราว์เซอร์ที่ถูกต้องทั่วไปโดยที่ผู้ใช้ไม่ทันได้เฉลียวใจ ซึ่งจะต่างจากผู้ใช้ Internet Explorer ที่ระบบจะนำผู้ใช้ไปยังแบบสำรวจทันที

และเมื่อพิจารณาการโจมตีนี้อย่างละเอียดแล้ว พบว่าโดยส่วนใหญ่จะถูกสร้างขึ้นในลักษณะของการแสร้งแสดงเป็นส่วนขยายของ *Chrome* ที่ถูกต้องทั่วไป ดังนั้น เราจึงสรุปได้ว่าผู้ใช้ Chrome กำลังตกเป็นเป้าหมายหลักของการโจมตีในครั้งนี้ ขณะที่การปรับเปลี่ยนเส้นทางของ IE ถือเป็นลำดับรองลงมา อย่างไรก็ตาม แม้ว่า TROJ_FOOKBACE.A อาจติดตามตรวจสอบกิจกรรมของเบราว์เซอร์ที่เกี่ยวข้อง แต่ดูเหมือนจะไม่ได้มีเทคนิคการ

โจรกรรมข้อมูลใดๆ มีลักษณะเหมือนกับการโจมตีที่เรียกว่า ClickJacking (การขโมยคลิก นั่นคือหลอกให้ผู้ใช้คลิกลิงก์บนเว็บ เพื่อให้ผู้ที่ไม่หวังดีสามารถผ่านเข้าไปควบคุมการทำงานในเครื่องคอมพิวเตอร์ของเหยื่อได้) มากกว่าโดยจะมีการ ‘ถูกใจ’ (like) หน้า *Facebook* หลายๆ หน้าโดยอัตโนมัติพร้อมทั้งโพสต์ข้อความบนวอลล์ของผู้ใช้ที่ติดเชื้ออย่างต่อเนื่องอีกด้วย

การโจมตีที่มุ่งเน้นไปที่ *Chrome* และ *Firefox* แสดงให้เห็นว่าอาชญากรไซเบอร์กำลังกำหนดเป้าหมายการโจมตีไปที่เบราว์เซอร์ที่รองรับการใช้งานส่วนขยายเป็นพิเศษ รวมทั้งเบราว์เซอร์ที่กำลังได้รับความนิยมมากขึ้นด้วย จะเห็นได้ว่าการโจมตีในรูปแบบนี้ไม่ใช่ครั้งแรก โดยเบราว์เซอร์ที่มีคุณสมบัติสนับสนุนการใช้งานส่วนขยายและกำลังตกเป็นเป้าหมายหลักของโจมตีอยู่ในขณะนี้ถือเป็นคำเตือนให้ทราบว่า สิ่งนี่อาจเป็นแนวโน้มที่องค์กรร้ายในอินเทอร์เน็ตจะดำเนินการอย่างต่อเนื่องในอนาคตอันใกล้นี้

บริษัทเทรนด์ไมโครพร้อมให้การปกป้องผู้ใช้งานจากการโจมตีนี้แล้วผ่านทางเทรนด์ไมโคร สมาร์ท โพรเทคชั่น เน็ตเวิร์ก (Trend Micro™ Smart Protection Network™) ที่สามารถตรวจพบไฟล์ที่เป็นอันตรายและบล็อก URL อันตรายที่เกี่ยวข้องทั้งหมดได้อย่างครอบคลุม