

เทรนต์ไม่โครเตือนผู้ใช้อินเทอร์เน็ตให้ระวังเว็บไซต์ แจกฟรีวิดีโอสตรีมมิ่งไอรอนแมน 3

บริษัท เทรนต์ไม่โคร อินคอร์ปอเรท (TYO: 4704) ผู้นำระดับโลกด้านการรักษาความปลอดภัยสำหรับระบบคลาวด์พบว่าจากกระแสความแรงของภาพยนตร์เรื่องไอรอนแมน 3 (Iron Man 3) มีเว็บไซต์นับร้อยแห่งบนอินเทอร์เน็ตได้ใช้ประโยชน์จากความดังของภาพยนตร์ทำเงินใน Box Office เรื่องนี้ โดยเมื่อเข้าเยี่ยมชมเว็บไซต์เหล่านี้ ผู้ใช้จะต้องดาวน์โหลดติดตั้งวิดีโอซึ่งจะไม่มีการเล่นภาพยนตร์เรื่องดังกล่าว แต่จะเป็นการเปิดช่องโหว่ให้กับมัลแวร์แทน นอกจากนี้แพลตฟอร์มสื่อสังคมออนไลน์ เช่น Facebook และบล็อกที่มีชื่อเสียงจำนวนมากก็ยังไม่อนุญาตให้อาชญากรไซเบอร์สามารถแพร่กระจายข่าวลวงของเว็บไซต์ที่ระบุข้อความว่า “Free Iron Man 3 Streaming Video” (แจกฟรีวิดีโอสตรีมมิ่งเรื่องไอรอนแมน 3) เพื่อดึงดูดให้ผู้ใช้เข้าไปทำแบบสำรวจที่สร้างผลประโยชน์ทางการเงินให้กับผู้หลอกลวงดังกล่าว

นายพอล โอลิเวอเรีย หัวหน้าฝ่ายซีเคียวริตีไฟกัส ศูนย์วิจัยเทรนต์แล็บส์ บริษัท เทรนต์ไม่โคร อินคอร์ปอเรท กล่าวว่า “ภาพยนตร์ทำเงินในช่วงซัมเมอร์อย่างเช่น ไอรอนแมน 3 ถูกใช้เป็นเหยื่อล่อในการก่ออาชญากรรมไซเบอร์ เนื่องจากสามารถล่อลวงให้ผู้ใช้เข้าไปเยี่ยมชมเว็บไซต์หลอกลวงที่จัดตั้งไว้ได้ เนื่องจากการใช้กลยุทธ์ด้านวิศวกรรมสังคมที่ฉลาดกว่าเดิม ผู้ใช้จึงอาจติดกับดักของวายร้ายเหล่านี้ได้ไม่ยาก ดังนั้นจึงเป็นสิ่งสำคัญที่จะทุกคนจะต้องทราบถึงวิธีการทำงานของวิศวกรรมสังคมและมีสติทุกครั้งที่คลิกและแชร์เรื่องราวต่างๆ บน Facebook รวมถึงบัญชีผู้ใช้สื่อสังคมออนไลน์อื่นๆ ของคุณด้วย”



รูปที่ 1. ครึ่งหนึ่งของเว็บไซต์ลวงเกี่ยวกับภาพยนตร์เรื่องไอรอนแมน 3 ใช้บริการจาก *Tumblr*

เทรนต์แล็บส์พบว่าเว็บไซต์ลวงไอรอนแมน 3 เกิดขึ้นก่อนที่จะมีการเปิดตัวภาพยนตร์เรื่องนี้เป็นทางการในประเทศสหรัฐอเมริกา โดยเว็บไซต์ส่วนใหญ่ได้เลือกใช้บริการบล็อกยอดนิยม (ครึ่งหนึ่งของเว็บไซต์ลวงไอรอนแมน 3 พบว่าใช้ Tumblr) เพื่อลวงให้ผู้ใช้ไปยังหน้าเว็บสำหรับดาวน์โหลดหรือสตรีมมิ่งปลอมของภาพยนตร์เรื่องไอรอนแมน 3

จากการวิเคราะห์ของเทรนต์แล็บส์พบว่าโปรแกรมเล่นวิดีโอที่ดาวน์โหลดมานั้นถูกระบุว่าเป็น “โปรแกรมเล่นวิดีโอที่ถูกต้อง” แต่เป็นที่ทราบกันดีว่าโปรแกรมเล่นวิดีโอนี้เคยเผยแพร่โฆษณาที่ก้าวร้าวมาแล้วในอดีต และไฟล์ที่ถูกต้องเหล่านี้สามารถถูกแทนที่ด้วยมัลแวร์ได้อย่างง่ายดายในเวลาต่อมา ดังนั้นจึงไม่น่าแปลกใจที่จะพบว่าหน้าเว็บสำหรับ

ดาวน์โหลดหรือสตรีมมิ่งหนังเรื่องไอรอนแมน 3 จึงเป็นที่โฮสต์มัลแวร์ไว้หลังจากนั้น

ไม่น่าแปลกใจที่อาชญากรไซเบอร์บางรายใช้ Facebook ในการแพร่กระจายลิงก์สตรีมมิ่งภาพยนตร์เรื่องไอรอนแมน 3 ฟรีด้วย โดยเมื่อผู้ใช้คลิกลิงก์ดังกล่าว ก็จะถูกนำไปยังหน้าเว็บหลายๆ หน้าที่มีแบบสำรวจ และเพื่อนๆ บน Facebook ของพวกเขาก็จะได้รับสแปมพร้อมโพสต์ในลักษณะเดียวกันนี้เช่นกัน ทั้งนี้เทรนต์แล็บส์พบว่ามีการหลอกลวงในลักษณะที่คล้ายกันนี้ในช่วงที่ผ่านมา ซึ่งรวมถึง **“Facebook Profile Viewer” (ตัวแสดงโปรไฟล์ Facebook)** และแบบสำรวจที่อ้างถึงการแข่งขัน **Google Glass**

เว็บไซต์เหล่านี้ไม่ได้นำไปสู่ภาพยนตร์โฆษณาเรื่องจริง แต่จะขอให้ผู้ใช้ลงทะเบียนและจะใส่หมายเลขบัตรเครดิตของพวกเขาซึ่งเป็นที่น่าสงสัยอย่างมาก

ทั้งนี้ บริษัท เทรนต์ ไมโคร ได้บล็อกเว็บไซต์และโดเมนที่เกี่ยวข้องกับภัยคุกคามนี้แล้ว สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเรื่องนี้สามารถดูได้ที่:

<http://blog.trendmicro.com/trendlabs-security-intelligence/fake-iron-man-3-streaming-sites-sprout-on-social-media/>