

ฉบับที่ 22,006 วันอังคารที่ 19 มิถุนายน พ.ศ. 2553 หน้า 12

InsuT

ไมโคร จัดอันดับ 10
ภัยร้ายออนไลน์ช่วง
เทศกาลวันหยุดปีใหม่ที่
ผ่านมามีทั้งคลิกลิงก์สแปม ลาวนัโหลด
ไฟล์ หลอกให้กรอกข้อมูลส่วนตัว รวมถึง
ส่วนต่อที่ไร้ชื่อของถูก

นายเจท โซเวียโน ฝ่ายสื่อสารด้าน
เทคนิค ศูนย์วิจัยข้อมูลเทรนต์แล็บส์ เปิดเผย
ว่า อาชญากรไซเบอร์จะใช้เทคนิคกลลวงทาง
สังคมที่แตกต่างกันเพื่อหลอกล่อเหยื่อ เช่น
การคลิกลิงก์ที่เป็นสแปม ลาวนัโหลดไฟล์
หรือการกรอกแบบฟอร์มโดยใส่ข้อมูลส่วนตัว
ที่เป็นความลับ สิ่งเหล่านี้จะก่อให้เกิดผล

ไว้ นอกจากผู้โจมตีที่ตอบกลับข้อความอีเมล
ทางหรือเว็บไซต์ลวงซึ่งไม่ได้ให้ความช่วยเหลือ
แก่ผู้ใดแล้ว ยังจะต้องสูญเสียเงินหรือข้อมูลที่เป็น
ความลับไปแทนอีกด้วย

อันดับ 8 บัตรรอยหรืออิเล็กทรอนิกส์
(อีการ์ด) : อาชญากรไซเบอร์มักจะใช้บัตร
ขายหรืออิเล็กทรอนิกส์ หรืออีการ์ดเพื่อล่อลวง
เหยื่อให้คลิกลิงก์ที่เป็นอันตรายในข้อความ
สแปม และนั่นอาจทำให้เครื่องคอมพิวเตอร์
ของเหยื่อตกอยู่ในอันตรายได้ การโจมตี
ประเภทนี้มักใช้ประโยชน์ของเทศกาลวันหยุด
เมื่อมีผู้ใช้ส่งอีการ์ดมากขึ้น และคาดหวังว่าอี
การ์ดที่ได้รับนั้นจะมาจากเพื่อนหรือญาติสนิท

พิษสืบสุดยอดภัยออนไลน์ช่วงปีใหม่

ประโยชน์ทางการเงินแก่อาชญากรไซเบอร์
ซึ่งพยายามจะหลอกล่อเหยื่อในช่วงเทศกาลวัน
หยุด เนื่องจากเป็นช่วงที่มีผู้ใช้งานอินเทอร์เน็ต
เน็ตเป็นจำนวนมาก ที่เข้าไปซื้อสินค้าและ
บริการผ่านเว็บไซต์

โดย เทรนต์ ไมโคร ได้จัดทำสรุป 10
อันดับภัยร้ายออนไลน์ที่ผู้ใช้งานอินเทอร์เน็ต
ในช่วงวันหยุด ดังนี้

อันดับ 10 ภัยลวงนักล่าของถูก :
อาชญากรไซเบอร์จะใช้ส่วนต่อและโปรโมชัน
เพื่อหลอกล่อเหยื่อให้คลิกลิงก์ที่เป็นอันตราย
หรือใส่ข้อมูลที่เป็นความลับของตนลงใน
เว็บไซต์หลอกลวง โดยทั่วไปแล้วผลิตภัณฑ์
ที่นำมาใช้ล่อเหยื่อจะเป็นสินค้าชอปปิงและ
สินค้าขายดี ซึ่งอาจทำให้ผู้ใช้เผลอใจไม่ได้ที่จะ
คลิกลิงก์ที่ปรากฏ และในปีที่เทรนต์ ไมโคร
พบว่าโทรจัน TROJ_AYFONE.A ใช้
ประโยชน์จากการเปิดตัวแอปเปิล ไอโฟน
โดยมัลแวร์จะแสดงในรูปแบบโฆษณาตวง
เหมือนกับการสร้างเว็บไซต์ลวงของร้านค้า
ออนไลน์ที่สามารถซื้อผลิตภัณฑ์ดังกล่าวได้

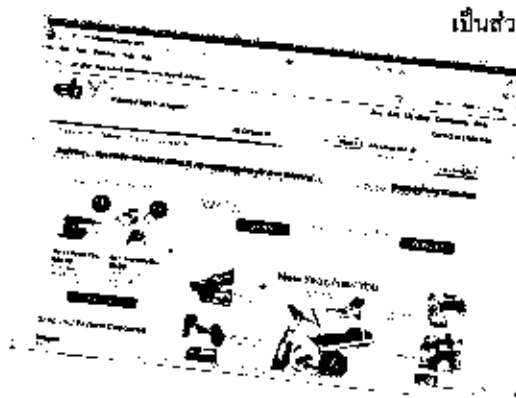
อันดับ 9 เว็บไซต์การกุศลจอมปลอม
ภัยพิบัติต่าง ๆ ที่เกิดขึ้นทั่วโลก เช่น เหตุ
การณ์แผ่นดินไหว ไฟป่า น้ำท่วม ล้วนถูก
อาชญากรไซเบอร์นำมาใช้ประโยชน์เพื่อ
หลอกลวง โดยเฉพาะเทศกาลวันหยุดเป็น
ช่วงเวลาที่ผู้ใช้อินเทอร์เน็ตเป็นส่วนใหญ่เกิด
ความรู้สึก "อยากทำบุญและต้องการบริจาค"
อยู่แล้ว ซึ่งมักเป็นช่วงเวลาที่ดีที่สุดสำหรับ
อาชญากรไซเบอร์ที่จะบรรจูดามแผนการที่วาง



อันดับ 7 โฆษณามัลแวร์ (Malver-
tisements) : อาชญากรไซเบอร์จะใช้โฆษณา
และโปรโมชันของปลอม (เลียนแบบโฆษณา
ของจริง) เพื่อแพร่กระจายมัลแวร์ โดยอาศัย
ความเชื่อใจของผู้ซื้อสินค้าออนไลน์ที่มัก
สนใจเรื่องสินค้าราคาพิเศษ โฆษณาที่แสดง
อยู่ในเว็บไซต์ที่มีการเข้าชมสูงจะถูกใช้เป็นตัว
กระตุ้นให้ดาวน์โหลดมัลแวร์ โดยเว็บไซต์
ชอปปิง เช่น Google, Expedia.com,
Rhapsody.com, Blick.com และแม้แต่
นิตยสารพีซ มักถูกใช้เป็นที่ฝังตัวของมัล
แวร์โฆษณาที่เป็นอันตราย ซึ่งเมื่อคลิกเข้าไป
ดูก็จะดาวน์โหลดมัลแวร์ลงในระบบของผู้ใช้
งานได้แสดงให้เห็นว่าโฆษณาที่เป็นอันตราย
เหล่านี้ถูกฝังตัวอยู่ในแทบจะทุกแห่งบนโลก
ไซเบอร์

อันดับ 6 ผลการค้นหาแหล่งขอบัง
ช่วงคริสต์มาส : ผลลัพธ์คำขอที่มากับ
สตรีปต์ที่เป็นอันตราย ทำให้เกิดภัยคุกคาม
หลากหลายรูปแบบ เช่น มัลแวร์ ฟิชชิงไซต์
ฮูอาร์แอดอันตราย โดยผู้เขียนมัลแวร์จะเลือก

ช่วงเทศกาลต่าง ๆ ที่จะนำผู้ใช้งานไปถึง ผลลัพธ์ที่เป็นอันตรายของคนได้ ในปี พ.ศ. 2550 ผลของการค้นหาคำว่า “Christmas



gift shopping” ถูกพบว่านำไปสู่มัลแวร์ หลากหลายชนิดที่เป็นอันตราย และเมื่อเร็ว ๆ นี้ ผลของการค้นหาคำว่า “Halloween costumes” ถูกพบว่าแอบซ่อนซอฟต์แวร์ ป้อนกัมไวรัสของปลอมไว้

อันดับ 6 เว็บไซต์สุดฮิต : จัดเป็นภัยคุกคามสำหรับผู้ใช้ออนไลน์ เพราะเป้าหมายหลักของการคิดเชื่อจะเกิดขึ้นบนเว็บไซต์ที่คาดว่าปลอดภัยและน่าเชื่อถือ โดยเฉพาะอย่างยิ่งช่วงวันหยุดเทศกาลที่กำลังจะมาถึง ซึ่งผู้ซื้อนิยมซื้อสินค้าผ่านทางออนไลน์ เช่น ร้านอาหารออนไลน์ เว็บไซต์ประมูล หรือเว็บไซต์อีคอมเมิร์ซ อาชญากรไซเบอร์จะแพร่กระจายเชื้อไปยังเหยื่อโดยการล่อลวงเว็บไซต์ช้อปนิยม และมีการเข้ารหัสสูง

อันดับ 4 ข้อมูลส่วนบุคคล - บัตรของขวัญและโปรโมชั่น (ของปลอม) : ผู้ใช้ที่ขอยกค้นหารหัสหรือโปรโมชั่นพิเศษบนเว็บนั้นเสี่ยงต่อการถูกโจมตีในลักษณะนี้ได้แบบสำรวจข้อมูลที่ดูเหมือนจะปลอดภัยกับนักจะถูกใช้เก็บข้อมูลส่วนบุคคล โดยของรางวัล

บัตรของขวัญ หรือแม้แต่เงินสดจะถูกใช้เพื่อ ล่อเหยื่อให้กรอกแบบสำรวจของโลกม โดยที่เหยื่อจะไม่ทราบว่ามันคือ ฟิชซิงไซด์ และเป็นส่วนหนึ่งของแผนการขโมยข้อมูลส่วนตัว ที่เป็นความลับ

อันดับ 3 อีคอมเมิร์ซฟิชซิง : อีเบย์ (eBay) ถูกจัดอันดับให้เป็นร้านค้าปลีกออนไลน์ที่ได้รับความนิยมสูงสุดในปี 2550 มีผู้ใช้บริการมากกว่า 124 ล้านคน และอีเบย์ยังคิดอันดับสูงสุดของเว็บไซต์ที่แสกเกอร์นิยมใช้ทำเป็นเว็บไซต์ลวงด้วย นับจากการขโมยข้อมูลส่วนบุคคล จนถึงการจัดอันดับความน่าเชื่อถือ อาชญากรไซเบอร์จะใช้แผนการที่ชาญฉลาด เพื่อให้ได้ข้อมูลของผู้ใช้เพื่อเพิ่มผลประโยชน์ทางการเงิน

อันดับ 2 โทรจันที่มาพร้อมใบรับสินค้า (ของปลอม) : ข้อความต่าง ๆ จากผู้จัดส่งสินค้าขอลนิคม ซึ่งแจ้งทางอีเมลว่าไม่สามารถส่งมอบของให้ผู้รับได้ พร้อมแนบไฟล์ข้อมูลที่ดูเหมือนเป็นใบแจ้งหนี้ แต่จริง ๆ แล้วเป็นข้อความสแปมที่จะล่อลวงผู้ใช้ให้ติดตั้งโทรจันลงในเครื่องคอมพิวเตอร์ ปัญหาดังกล่าวค่อนข้างแยกแยะลำบากสำหรับนักช้อปออนไลน์ที่กำลังรอการจัดส่งสินค้าในช่วงเทศกาล ทั้งนี้ยูทูป และ เฟดเดกซ์ เป็นตัวอย่างของบริษัทผู้จัดส่งสินค้าที่อาชญากรไซเบอร์นิยมใช้เป็นเหยื่อล่อผู้ซื้อสินค้าออนไลน์มากที่สุด

อันดับ 1 โบนักราคาสินค้า (ปลอม): บางครั้งผู้ใช้งานอาจจะได้รับข้อความอีเมลที่แจ้งให้พวกเขาเปิด และพิมพ์ “โบนักราคาสินค้า” ที่ได้แนบมา ไฟล์ที่แนบมานั้นไม่ใช่โบนักราคาสินค้าของจริง แต่ว่าเป็นโทรจัน ผู้ที่ซื้อสินค้าออนไลน์บ่อย ๆ จะได้รับโบนักราคาสินค้าอยู่แล้ว และถือเป็นการเป้าหมายหลักของภัยคุกคามประเภทนี้ แต่ในทางกลับกันผู้ใช้ที่ไม่เคยซื้อสินค้าออนไลน์ และมั่นใจว่าไม่ได้ทำการสั่งซื้อสินค้าใด ๆ ก็อาจจะสงสัยและเปิดไฟล์แนบท้ายดังกล่าว สแปมก็จะแพร่กระจายไปทั่ว ล่าสุดที่พบคือ หนอนไวรัส WORM_OTORUN.C ดังนั้นผู้ใช้อินเทอร์เน็ตหรือผู้ซื้อสินค้าออนไลน์จึงต้องระมัดระวังและทำเนิ่งถึงความปลอดภัยมากขึ้นระหว่างเลือกซื้อสินค้าออนไลน์.