10 ภัยร้ายออนไลน์...ที่ต้องระวังช่วงเทศกาลวันหยุด!!!!

นำเสนอเมื่อ : 20 ธ.ค. 2552

ก่อนจะถึงเทศกาลหยุดงานแสนสบายใจ ไปดูสรุป 10 อันดับภัยร้ายออนไลน์ที่ชาวไอทีทุกคนต้องระวังตัวในช่วงเทศกาลวันหยุด

ภัยร้าย 10 อันดับนี้เรียบเรียงโดยนายเจค โซเรียโน ฝ่ายสื่อสารด้านเทคนิค ศูนย์วิจัยข้อมูลเทรนด์แล็บส์
เพื่อให้ทุกคนไม่หลงกลอาชญากรไซเบอร์ที่จะใช้เทคนิคกลลวงทางสังคมที่แตกต่างกันเพื่อหลอกล่อชาวเน็ตที่พากันค้นหาร้านค้าและเลือกซื้อสินค้าออนไลน์มากกว่าปกติ เช่น การคลิกลิงค์ที่เป็นสแปม, การดาวน์โหลดไฟล์ หรือการกรอกแบบฟอร์มโดยใส่ข้อมูลส่วนตัวที่เป็นความลับ

อันดับ 10 - ภัยลวงนักล่าของถูก:
อาชญากรไซเบอร์จะใช้ส่วนลดและโปรโมชันเพื่อหลอกล่อเหยื่อให้คลิกลิงก์ที่เป็นอันตราย หรือใส่ข้อมูลที่เป็นความลับของตนลงในเว็บไซต์หลอกลวง

โดยทั่วไปแล้วผลิตภัณฑ์ที่นำมาใช้ล่อเหยื่อจะเป็นสินค้ายอดนิยมและสินค้าขายดี ซึ่งอาจทำให้ผู้ใช้อดใจไม่ได้ที่จะคลิกลิงก์ที่ปรากฏ เช่นในปีนี้เทรนด์ ไมโคร พบว่าโทรจัน TROJ_AYFONE.A ใช้ประโยชน์จากการเปิดตัว Apple iPhone
โดยมัลแวร์จะแสดงในรูปแบบโฆษณาลวงเหมือนกับการสร้างเว็บไซต์ลวงของร้านค้าออนไลน์ที่สามารถซื้อผลิตภัณฑ์ดังกล่าวได้

อันดับ 9 - ไซต์การกุศลจอมปลอม: ภัยพิบัติต่างๆ ที่เกิดขึ้นทั่วโลก เช่น เหตุการณ์แผ่นดินไหว ไฟป่า น้ำท่วม ล้วนถูกอาชญากรไซเบอร์นำมาใช้ประโยชน์เพื่อหลอกลวง
โดยเฉพาะเทศกาลวันหยุดเป็นช่วงเวลาที่ผู้ใช้อินเทอร์เน็ตส่วนใหญ่เกิดความรู้สึก "อยากทำบุญและต้องการบริจาค"

เทศกาลปีใหม่จึงเป็นช่วงเวลาที่ดีที่สุดสำหรับอาชญากรไซเบอร์ที่จะบรรลุตามแผนการที่วางไว้ นอกจากผู้ใจบุญที่ตอบกลับข้อความอีเมลลวงหรือเว็บไซต์ลวงซึ่งไม่ ได้ให้ความช่วยเหลือแก่ผู้ใดแล้ว

ยังจะต้องสูญเสียเงินหรือข้อมูลที่เป็นความลับไปแทนอีกด้วย

อันดับ 8 – บัตรอวยพรอิเล็กทรอนิกส์ (อี-การ์ด):
อาชญากรไซเบอร์มักจะใช้บัตรอวยพรอิเล็กทรอนิกส์
หรืออีการ์ดเพื่อลอลวงเหยื่อให้คลิกลิงก์ที่เป็นอันตรายในข้อความสแปม
และนั่นอาจทำให้เครื่องคอมพิวเตอร์ของเหยื่อตกอยู่ในอันตรายได้

การโจมตีประเภทนี้มักใช้ประโยชน์ของเทศกาลวันหยุด เมื่อมีผู้ใช้ส่งอีการ์ดมากขึ้น
และคาดหวังว่าอีการ์ดที่ได้รับนั้นจะมาจากเพื่อนหรือญาติสนิท

อันดับ 7 - โฆษณามัลแวร์ (Malvertisements):
อาชญากรไซเบอร์จะใช้โฆษณาและโปรโมชันของปลอม (เลียนแบบโฆษณาของจริง) เพื่อแพร่กระจายมัลแวร์
โดยอาศัยความเชื่อใจของผู้ซื้อสินค้าออนไลน์ที่มักสนใจเรื่องสินค้าราคาพิเศษ

โฆษณาที่แสดงอยู่ในเว็บไซต์ที่มีการเข้าชมสูงจะถูกใช้เป็นตัวกระตุ้นให้ดาวน์โหลด มัลแวร์
โดยเว็บไซต์ยอดนิยม เช่น Google, Expedia.com, Rhapsody.com, Blick.com และแม้แต่ MySpace
มักถูกใช้เป็นที่แฝงตัวของแบนเนอร์โฆษณาที่เป็นอันตราย
ซึ่งเมื่อคลิกเข้าไปดูก็จะดาวน์โหลดมัลแวร์ลงในระบบของผู้ใช้งานได้แสดงให้เห็นว่าโฆษณาที่เป็นอันตรายเหล่านี้ถูก
ฝังตัวอยู่ในแทบจะทุกแห่งบนโลกไซเบอร์

อันดับ 6 - ผลการค้นหาแหล่งช้อปปิ้งช่วงคริสต์มาส (ที่เป็นอันตราย):
ผลลัพธ์คำตอบที่มากับสคริปต์ที่เป็นอันตราย ทำให้เกิดภัยคุกคามหลากหลายรูปแบบ เช่น มัลแวร์ ฟิชชิ่งไซต์
ยูอาร์แอลอันตราย โดยผู้เขียนมัลแวร์จะเลือกช่วงเทศกาลต่างๆ
ที่จะนำผู้ใช้งานไปยังผลลัพธ์ที่เป็นอันตรายของตนได้

ในปี 2550 ผลของการค้นหาคำว่า "Christmas gift shopping"
ถูกพบว่านำไปสู่มัลแวร์หลากหลายชนิดที่เป็นอันตราย และเมื่อเร็วๆ นี้ ผลของการค้นหาคำว่า "Halloween
costumes" ถูกพบว่าแอบซอนซอฟต์แวร์ป้องกันไวรัสของปลอมไว้

อันดับ 5 - เว็บไซต์สุดฮิต: จัดเป็นภัยคุกคามสำหรับผู้ใช้ออนไลน์
เพราะเป้าหมายหลักของการติดเชื้อจะเกิดขึ้นบนเว็บไซต์ที่คาดว่าปลอดภัยและน่าเชื่อถือ
โดยเฉพาะอย่างยิ่งช่วงวันหยุดเทศกาลที่กำลังจะมาถึง ซึ่งผู้ซื้อนิยมซื้อสินค้าผ่านทางออนไลน์ เช่น
ร้านอาหารออนไลน์ เว็บไซต์ประมูล หรือเว็บไซต์อีคอมเมิร์ซ

อาชญากรไซเบอร์จะแพร่กระจายเชื้อไปยังเหยื่อโดยการเลือกเว็บไซต์ยอดนิยม และมีการเข้าชมสูง

อันดับ 4 - ข้อมูลส่วนบุคคล – บัตรของขวัญและโปรโมชัน (ของปลอม):
ผู้ใช้ที่ชอบค้นหาของฟรีหรือโปรโมชันพิเศษบนเว็บนั้นเสี่ยงต่อการถูกโจมตีในลักษณะนี้ได้
แบบสำรวจข้อมูลที่ดูเหมือนจะปลอดภัยนี้มักจะถูกใช้เก็บข้อมูลส่วนบุคคล

ของรางวัล บัตรของขวัญ หรือแม้แต่เงินสดจะถูกใช้เพื่อล่อเหยื่อให้กรอกแบบสำรวจของปลอม
โดยที่เหยื่อจะไม่ทราบว่านั่นคือ ฟิชชิ่งไซต์ และเป็นส่วนหนึ่งของแผนการขโมยข้อมูลส่วนตัวที่เป็นความลับ

อันดับ 3 - อีคอมเมิร์ซฟิชชิ่ง: อีเบย์ (eBay)
ถูกจัดอันดับให้เป็นร้านค้าปลีกออนไลน์ที่ได้รับความนิยมสูงสุดในปี 2550 มีผู้ใช้บริการมากกว่า 124 ล้านคน
และอีเบย์ยังติดอันดับสูงสุดของเว็บไซต์ที่แฮคเกอร์นิยมใช้ทำเป็นเว็บไซต์ลวงด้วย
นับจากการขโมยข้อมูลส่วนบุคคลจนถึงการจัดอันดับความน่าเชื่อถือ

อาชญกรไซเบอร์จะใช้แผนการที่ชาญฉลาดเพื่อให้ได้ข้อมูลของผู้ใช้เพื่อเพิ่มผลประโยชน์ทางการเงิน

อันดับ 2 - โทรจันที่มาพร้อมใบรับสินค้า (ของปลอม): ข้อความต่างๆ
จากผู้จัดส่งสินค้ายอดนิยม ซึ่งแจ้งทางอีเมลว่าไม่สามารถส่งมอบของให้ผู้รับได้
พร้อมแนบไฟล์ข้อมูลที่ดูเหมือนเป็นใบแจ้งหนี้ แต่จริงๆ แล้วเป็นข้อ
ความสแปมที่จะล่อลวงผู้ใช้ให้ติดตั้งโทรจันลงในเครื่องคอมพิวเตอร์

ปัญหาดังกล่าวค่อนข้างแยกแยะลำบากสำหรับนักช้อปออนไลน์ที่กำลังรอการจัดส่งสินค้าในช่วงเทศกาล ทั้งนี้
UPS และ FedEx
เป็นตัวอย่างของบริษัทผู้จัดส่งสินค้าที่อาชญากรไซเบอร์นิยมใช้เป็นเหยื่อล่อผู้ซื้อสินค้าออนไลน์มากที่สุด

อันดับ 1 – ใบแจ้งราคาสินค้า (ปลอม):
บางครั้งผู้ใช้งานอาจจะได้รับข้อความอีเมลที่แจ้งให้พวกเขาเปิด และพิมพ์ “ใบแจ้งราคาสินค้า” ที่ได้แนบมา
ไฟล์ที่แนบมานั้นไม่ใช่ใบแจ้งราคาสินค้าของจริง แต่ว่าเป็นโทรจัน ผู้ที่ซื้อสินค้าออนไลน์บ่อยๆ
จะได้รับใบแจ้งราคาสินค้าอยู่แล้ว และถือเป็นเป้าหมายหลักของภัยคุกคามประเภทนี้

แต่ในทางกลับกันผู้ใช้ที่ไม่เคยซื้อสินค้าออนไลน์ และแน่ใจว่าไม่ได้ทำการสั่งซื้อสินค้าใดๆ
ก็อาจจะสงสัยและเปิดไฟล์แนบท้ายดังกล่าว สแปมก็จะแพร่กระจายไปทั่ว ล่าสุดที่พบคือหนอนไวรัส
WORM_OTORUN.C ดังนั้นผู้ใช้อินเทอร์เน็ตหรือ
ผู้ซื้อสินค้าออนไลน์จึงต้องระมัดระวังและคำนึงถึงความปลอดภัยมากขึ้นระหว่างเลือกซื้อสินค้าออนไลน์

สรุปคือ ด้วยปริมาณและความสามารถของภัยคุกคามข้อมูลที่เพิ่มขึ้น
ผู้ใช้งานจึงจำเป็นที่จะต้องมีการป้องกันข้อมูลแบบหลายระดับชั้น
เพื่อเพิ่มความมั่นใจในการใช้งานอินเทอร์เน็ตได้อย่างปลอดภัยมากขึ้น เทรนด์
ไมโครจึงได้นำเสนอเทคโนโลยีเครือข่ายป้องกันภัยอัจฉริยะ (สมาร์ท โพรเทคชัน เน็ตเวิร์ค)
ที่ช่วยปกป้องผู้ใช้งานจากภัยคุกคามต่างๆ อาทิ สแปม หรือยูอาร์แอลที่เป็นอันตราย

และไฟล์อันตรายต่างๆ ด้วยจำนวนและความสามารถของภัยคุกคามทางเว็บที่เกิดขึ้น ทำให้เราจำเป็นที่จะต้องมีการปกป้องข้อมูลแบบหลายระดับชั้น และทันท่วงที ถ้าผู้ซื้อสินค้าออนไลน์ต้องการได้รับความปลอดภัยจากการดำเนินกิจกรรมต่างๆ ผ่านทางออนไลน์

http://www.manager.co.th/CyberBiz/ViewNews.aspx?NewsID=9520000155312