แคสเปอร์สกี้ แลป พบสแปมเมอร์อาศัยเกาะกระแส WannaCry หาเงิน

ไตรมาสที่ 2 ปี 2017 อาชญากรที่เกี่ยวโยงกับการแพร่กระจายสแปมได้มีความพยายามที่จะแพร่กระแสความหวาดกลัว โดยเกาะวิกฤตแรนซัมแวร์ WannaCry ระบาดเมื่อเดือนพฤษภาคมที่ผ่านมา รู้อยู่แก่ใจดีว่ามีช่องโหว่ที่เหยื่อพยายามจะพยายามทุกวิถีทางที่จะแกะรหัส เพื่อกู้ข้อมูลกลับคืนมาให้ได้ จึงเป็นช่องให้คนโกงเหล่านี้สบโอกาสส่งอีเมลสแปมหรือฟิชชิ่งออกมานำเสนอบริการอ้างว่าสามารถที่จะป้องกันรับมือการระบาดของแรนซัมแวร์ได้ ตัวอย่างนี้เป็นหนึ่งในข้อมูลในรายงานการสำรวจ “สแปมและฟิชชิ่ง ไตรมาส 2 ปี 2017”

การโจมตีแรนซัมแวร์ WannaCry ทำให้เครื่องคอมพิวเตอร์ติดเชื้อมากกว่า 200,000 เครื่องทั่วโลกยังผลให้เกิดความตื่นตระหนกโกลาหลไปทั่ว และสแปมเมอร์ก็ได้โอกาสครั้งใหญ่ นักวิจัยตรวจพบเมสเสจข้อความจำนวนมากที่นำเสนอบริการ อาทิ ป้องกันให้พ้นภัย WannaCry การกู้คืนข้อมูล และยิ่งน่าสะพรึงไปกว่านั้น เวิร์กช็อปให้การอบรม คอร์สการฝึกอบรมแก่ผู้ใช้งานคอมพิวเตอร์ นอกจากนั้น สแปมเมอร์ยังได้ติดตั้งดำเนินแผนการฉ้อโกงเป็นผลสำเร็จที่จะคอยทำหน้าที่เสนอบริการติดตั้งซอฟต์แวร์อัพเดทให้บนเครื่องที่เป็นเหยื่อมาแล้วอีกด้วย อย่างไรก็ตาม ลิ้งก์เหล่านี้ หากคลิ้กไปก็จะนำไปยังฟิฟิชชิ่งเพจ ที่ซึ่งคอยโจรกรรมข้อมูลส่วนตัวของเหยื่อที่หลงเข้ามา

หนึ่งในแนวทางหลักในช่วงสามเดือนที่ผ่านมาคือจำนวนอีเมลมากมายมหาศาลไปมีเป้าหมายไปยังระบบเครือข่ายคอร์ปอเรทต่างๆ จากการวิจัยข้อมูลโดยแคสเปอร์สกี้ แลป พบว่า กิจกรรมเช่นนี้ได้ขยายวงกว้างขึ้นตั้งแต่ต้นปี โดยพบว่าสแปมเมอร์เริ่มที่จะหลบเลี่ยงอีเมลให้ดูคล้ายบทสนทนาของกิจกรรมการดำเนินงานของคอร์ปอเรท ด้วยการใช้ไอเด็นติตี้ของคอร์ปอเรทนั้น ใช้ลายเซ็นจริง โลโก้จริง และแม้กระทั่งข้อมูลธนาคารก็ตาม ก็ดูเหมือนจริง ส่วนเอกสารที่ส่งแนบมากับอีเมลนั้น อาชญากรไซเบอร์ก็จะส่ง exploit packages เพื่อโจรกรรม FTP อีเมล และพาสเวิร์ดรหัสผ่านอื่นๆ ผู้เชี่ยวชาญของแคสเปอร์สกี้ แลปเน้นว่า การโจมตีคอร์ปอเรทส่วนมากนั้นจะมีเป้าหมายอยู่ที่การเงิน

นอกไปจากนี้ ในไตรมาสที่สองของปีนี้ นักวิจัยได้ตรวจพบว่ามีอัตราการเติบโตของการส่งอีเมลที่มีโทรจันแนบด้วย ใช้วิธีการส่งในนามผู้ให้บริการขนส่งต่างประเทศ สแปมเมอร์ส่งรายงานความคืบหน้าในการส่งสินค้า ด้วยข้อมูลพัสดุที่ไม่มีอยู่จริง เพราะประสงค์ที่จะโจรกรรมข้อมูลส่วนบุคคล หรือแพร่เชื้อไปตามเครื่องคอมพิวเตอร์ อาชญากรไซเบอร์จึงใช้วิธีการแพร่การะจายดาวน์โหลดลิ้งก์ที่มีมัลแวร์ แบ้งกิ้งโทรจัน Emotet ซึ่งพบเป็นครั้งแรกเมื่อปี พ.ศ. 2557 ในภาพรวมแล้ว พบว่าจำนวนของอีเมลที่มีเชื้อมัลแวร์แฝงอยู่นั้นเพิ่มขึ้นถึง 17% จากรายงานการวิจัยล่าสุดโดยแคสเปอร์สกี้ แลป

ดารยา กู้ดโคว่า ผู้เชี่ยวชาญการวิเคราะห์สแปม แคสเปอร์สกี้ แลป กล่าวว่า “ช่วงไตรมาสที่สองของปีนี้ เราพบแนวโน้มการเติบโตอย่างต่อเนื่องของสแปมและฟิชชิ่ง อาศัยกระแสความตื่นกลัว WannaCry ในการส่งอีเมลหว่านออกไปหาเหยื่อ แสดงว่าอาชญากรไซเบอร์นั้นให้ความสนใจในเรื่องกระแสต่างๆ เป็นพิเศษ และเกาะกระแสที่ได้รับความสนใจในระดับโลก ยิ่งไปกว่านั้น อาชญากรไซเบอร์ได้เริ่มที่จะหันมาให้ความสนใจในภาคส่วนธุรกิจต่อธุรกิจ หรือ B2B เพราะเห็นปริมาณเงินชัดเจน เราคาดว่าแนวโน้มนี้จะดำเนินต่อไปอีก และจำนวนและรูปแบบการจู่โจมคอร์ปอเรทมีแต่จะขยายตัวขึ้น”

แนวโน้มทิศทางและสถิติในไตรมาส 2 ที่น่าสนใจ ที่ทางนักวิเคราะห์ของแคสเปอร์สกี้ แลป ให้ความสนใจเป็นพิเศษ ได้แก่:

• จำนวนเฉลี่ยของสแปมเพิ่มจำนวนขึ้น 56.97% เวียดนามเป็นแหล่งสุดฮอตของสแปม แซงอเมริกาและจีนไปแล้ว ประเทศ 10 อันดับแรก ได้แก่ รัสเซีย บราซิล ฝรั่งเศส อิหร่าน และเนเธอร์แลนด์

• Necurs botnet ยังคงไม่ตายและยังอยู่ดี อย่างไรก็ตาม ผู้เชี่ยวชาญสังเกตว่าจำนวนสแปมที่ส่งออกมาจากบอตเน็ตนี้ลดน้อยลง และเริ่มไม่เสถียร

• ประเทศที่ตกเป็นเป้าหมายการจู่โจมของเมล์หว่าน (mailshots) คือ เยอรมันนี ส่วนประเทศที่เคยติดอันดับ ได้แก่ จีน นั้นไตรมาสนี้มาเป็นที่สอง ตามด้วยสหราชอาณาจักร ญี่ปุ่น และรัสเซีย เป้าหมายอื่นที่เป็นที่นิยมเช่นกัน ได้แก่ บราซิล อิตาลี เวียดนาม ฝรั่งเศส และสหรัฐอเมริกา

• ระบบต่อต้านฟิชชิ่งของแคสเปอร์สกี้ แลปได้รับการกระตุ้นให้ทำงาน 46,557,343 ครั้งบนคอมพิวเตอร์ของผู้ใช้แคสเปอร์สกี้ แลป บราซิลมีอัตราส่วนของเหยื่อสูงที่สุดที่ (18.09%) โดยรวมแล้ว มีผู้ที่ใช้ผลิตภัณฑ์ของแคสเปอร์สกี้ แลป ทั่วโลกถูกจู่โจมด้วยฟิชชิ่ง 8.26%

• ในไตรมาสที่ 1 เป้าหมายหลักของการจู่โจมด้วยฟิชชิ่งนั้นยังคงเป็นเช่นเดิม และเป็นกลุ่มการเงิน อาทิ ธนาคาร บริการชำระเงิน และร้านค้าออนไลน์

ซิลเวีย อึง ผู้จัดการทั่วไป แคสเปอร์สกี้ แลป ภูมิภาคเอเชียตะวันออกเฉียงใต้ กล่าวว่า “ทุกวันนี้ ประสิทธิภาพในการป้องกันนั้นขึ้นอยู่กับความยืดหยุ่นและความเสถียรของระบบที่มีศักยภาพในการเรียนรู้ด้วยตนเองได้ (self-learning systems) ที่รังสรรค์โดยผู้เชี่ยวชาญ และความสำเร็จในการป้องกันตนเองก็จะเป็นของผู้ที่สามารถที่จะทำการผสมผสาน (i) ความสามารถในการคำนวณ และ (ii) โครงสร้างที่มีความซับซ้อนที่รองรับการพัฒนาอัลกอริธึ่มใหม่ๆ ได้ และเราเรียกส่วนผสมของสิ่งเหล่านี้ว่า อัจฉริยภาพของฮิวแมนชีน-มนุษย์และมาชีน (Humachine Intelligence) – ส่วนผสมที่ลงตัวของสิ่งพื้นฐาน 3 ส่วน ได้แก่ บิ๊กดาต้า การเรียนรู้ของแมชชีน และความเชี่ยวชาญในการคิดวิเคราะห์ของมนุษย์”

แคสเปอร์สกี้ แลปแนะนำให้ผู้ใช้คอมพิวเตอร์ตามบ้านติดตั้งโซลูชั่นเพื่อความปลอดภัยที่เชื่อถือได้ เพื่อตรวจจับและบล็อกสแปมและฟิชชิ่ง เช่น โซลูชั่น Kaspersky Total Security

ธุรกิจต่างๆ ก็เช่นกันที่ควรที่จะติดตั้งโซลูชั่นเพื่อความปลอดภัย ที่มีฟังก์ชั่นเฉพาะตัวสำหรับจัดการกับไฟล์แนบที่มีเชื้อร้ายแฝงมาด้วยโดยเฉพาะ ธุรกิจขนาดย่อมก็สามารถที่จะป้องกันธุรกิจของตัวเองได้เช่นเดียวกับธุรกิจขนาดใหญ่ด้วยโซลูชั่น Kaspersky Small Office Security, Kaspersky Endpoint Security Cloud ซึ่งคอยตรวจจับ บล็อกอีเมลที่แฝงสแปมมาด้วย

บริษัทที่มีขนาดใหญ่ขึ้นมาสามารถที่จะใช้ประโยชน์จากการสแกนข้อความทั้งหมดเพื่อต่อต้านสแปมแฝงด้วยฟีเจอร์แบบเรียลไทม์บนคลาวด์บน Microsoft® Exchange และอีเมลเซิร์ฟเวอร์แบบลีนุกซ์ ด้วยแอพพลิเคชั่น Kaspersky Security for Mail Server ที่มาพร้อมกับ Kaspersky Total Security for Business