ปี 2561 Kaspersky Lab บล็อกกว่า 30 ล้านภัยคุกคามออนไลน์ในประเทศไทย ช่วย 3 ใน 10 ของผู้ใช้งานอินเทอร์เน็ตในไทยไม่ให้ถูกคุกคาม

Kaspersky Lab เปิดตัว Kaspersky Security Bulletin ของปี 2562 ด้วยสถิติภาพรวมภัยคุกคามในประเทศไทยของปีที่แล้ว รายงานระบุว่าอินเทอร์เน็ตยังคงเป็นหนึ่งในแหล่งของภัยคุกคามทางไซเบอร์ในประเทศ บริษัทให้บริการป้องกันด้านความปลอดภัยด้านอินเทอร์เน็ตระดับโลกได้ควบคุมหรือตรวจจับภัยทางอินเทอร์เน็ตได้ถึง 30,203,943 ชนิดในประเทศไทย

รายงานจากข้อมูลของ Kaspersky Security Network (KSN) ระบุว่าเมื่อปี 2561 ผู้ใช้งานอินเทอร์เน็ตของไทยกว่า 31.8% ได้ถูกโจมตีโดยภัยคุกคามทางอินเทอร์เน็ต ซึ่งมีอัตราการเพิ่มขึ้นอย่างชัดเจนจากปี 2560 ที่ Kaspersky Lab ได้ตรวจจับภัยคุกคามทางอินเทอร์เน็ตได้เพียง 12,696,011 ชนิด และมีผู้ใช้ที่ได้รับการโจมตีเพียง 29.0%

มร.ซูกูรุ อิชิมารุ นักวิจัยด้านความปลอดภัยของ Kaspersky Lab ประเทศญี่ปุ่น เปิดเผยว่า การเพิ่มขึ้นของภัยคุกคามออนไลน์ในประเทศไทยล้อตามเทรนด์ทั่วโลก ด้วยอัตราการเติบโตโดยภาพรวมของการติดตั้งของแพคเกจภัยคุกคามที่เป็นอันตราย และโทรจัน ที่อันตรายต่อการทำธุรกรรมทางการเงินหรือธนาคารบนมือถือหลาย ๆ ประเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้ กำลังกลายเป็นประเทศติดอันดับท็อปเท็นในโลกที่มีอัตราการถูกโจมตีจากภัยคุกคามทางอินเทอร์เน็ตสูง ตัวอย่างเช่น โทรจันของการทำธุรกรรมทางการเงินบนมือถือที่ชื่อว่า DanaBot ได้ถูกตรวจจับเมื่อไตรมาสที่ 2 ปี 2561 และยังเพิ่มขึ้นและพัฒนาขยายอย่างรวดเร็ว

“ปัจจุบันนี้ ประเทศไทยจัดอยู่ในอันดับที่ 73 ของโลกที่จัดอันดับจากระดับอันตรายจากภัยคุกคามทางอินเทอร์เน็ตที่เราได้ตรวจจับจากผู้ใช้งานอินเทอร์เน็ต ถึงแม้ว่าจะถือได้ว่าประเทศไทยเป็นประเทศที่ปลอดภัยกว่าประเทศอื่น ๆ ในภูมิภาคเดียวกัน แต่ทางเราก็ยังคงกระตุ้นให้ผู้ใช้งานอินเทอร์เน็ตในประเทศใช้การป้องกันความปลอดภัยจากภัยคุกคามทางอินเทอร์เน็ต จากการที่เราได้ป้องกันกว่า 30 ล้านชนิด เมื่อปีที่แล้ว พิสูจน์ได้ว่าประเทศไทยยังคงเป็นเป้าหมายของการโจรกรรมทางไซเบอร์ ดังนั้นควรจะเสริมเกราะป้องกันและเปลี่ยนนิสัยการใช้งานอินเตอร์เน็ต อย่าตกเป็นเหยื่อโดยไม่รู้ตัว” มร. โย เซียง เทียง ผู้จัดการทั่วไป Kaspersky Lab ภูมิภาคเอเชียตะวันออกเฉียงใต้

การโจมตีผ่านเบราเซอร์เป็นวิธีการหลักของการโจรกรรมที่เผยแพร่โปรแกรมที่อันตราย อาชญากรรมไซเบอร์ส่วนใหญ่จะหาช่องโหว่ของเบราเซอร์และปลั๊กอินด้วยการให้ดาวน์โหลด การติดไวรัสจะเกิดขึ้นเมื่อมีผู้เข้าชมเว็บไซต์ที่มีไวรัสโดยที่ไม่มีการป้องกันหรือผู้ใช้ไม่มีความรู้มาก่อน

กลวิธีนี้ใช้โจมตีกันอย่างแพร่หลาย ซึ่งมัลแวร์ที่ไม่มีไฟล์ (File-less) จะอันตรายที่สุด มันจะตั้งรหัสที่เป็นอันตรายต่อผู้ใช้หรือ WMI การสมัครรับข้อมูล ทำให้ไม่เหลือข้อมูลใด ๆ บนดิสก์เลย
สินค้าของ Kaspersky Lab ที่ได้พัฒนาเพื่อต่อสู้กับภัยคุกคามต่างๆ ที่หลบซ่อนอยู่ ใช้องค์กระกอบในการตรวจจับที่เรียกว่า Behavior Detection ที่เป็นประโยชน์จากต้นแบบ ML-based และการตรวจสอบพฤติกรรมที่เป็นอันตรายต่าง ๆ ถึงแม้ว่าไม่ทราบรหัสก็ตาม อีกหนึ่งเทคโนโลยีสำคัญที่พัฒนาโดย Kaspersky Lab ก็คือ Exploit Prevention ที่จะเปิดเผยและบล็อกมัลแวร์ในทันทีเมื่อเจอมัลแวร์ที่อาศัยช่องโหว่ของซอฟต์แวร์
การโจมตีทางออนไลน์อีกรูปแบบหนึ่ง เป็นแบบทั่วไปที่ต้องการให้ผู้ใช้มีส่วนร่วม นั่นคือ ผู้ใช้ต้องดาวน์โหลดไฟล์ที่เป็นอันตรายมาไว้ในคอมพิวเตอร์ จะเกิดขึ้นเมื่ออาชญากรไซเบอร์ทำให้เหยื่อเชื่อว่าพวกเขากำลังดาวน์โหลดโปรแกรมที่ถูกกฎหมายอยู่
เป้าหมายหลักของอาชญากรจะต้องทำให้ผู้ใช้ดาวน์โหลดมัลแวร์อันตรายเหล่านั้น ซึ่งเป็นโปรแกรมหรือแอปที่เป็นตัวที่จะขโมยข้อมูลต่าง ๆ มัลแวร์นี้สามารถปลอมตัวเป็นแอปอะไรก็ได้ไม่ว่าจะเป็นเกมส์ที่กำลังนิยมหรือแอปที่ใช้ตรวจสภาพอากาศหรือการจราจร ซึ่งไม่ควรที่จะเปิดอีเมลที่น่าสงสัย เช่นการแข่งขันหรือข้อเสนอที่ไม่น่าจะเป็นไปได้
ข้อแนะนำที่เป็นประโยชน์ จากทีมผู้เชี่ยวชาญด้านความปลอดภัยของ Kaspersky Lab ที่จะช่วยปกป้องเงินและข้อมูลของคุณเมื่อคุณออนไลน์

• อย่าคิดไปเองว่าลิ้งค์จะปลอดภัย
คุณควรจะพิมพ์ URL ด้วยตัวเอง แทนที่จะคลิกจากลิ้งค์ อย่าเข้าชมเว็บไซต์ที่คลิกเข้าไปจากอีเมล ข้อความหรือจากโซเชียล เน็ตเวิร์ก ต่าง ๆ ข้อความจากห้องแชท แบนเนอร์โฆษณาที่เป็นเว็บไซต์ที่น่าสงสัย ลิ้งค์ต่าง ๆ ที่ส่งมาจากคนที่คุณไม่รู้จัก

• ระวังการสื่อสารปลอม
องค์กรส่วนใหญ่จะไม่ขอให้ลูกค้าส่งข้อมูลส่วนตัวทางอีเมล หรือต้องขออนุมัติในการเข้าเยี่ยมชมเว็บไซต์ขององค์กรและใส่ข้อมูลส่วนตัวในหน้าต่าง pop-up

• ตรวจสอบ URL
เมื่อคุณเข้าเว็บไซต์ที่จำเป็นต้องกรอกข้อมูลส่วนตัวที่สำคัญ ให้ตรวจสอบดูที่อยู่ URL ว่าตรงกับเว็บไซต์ที่เราต้องการหรือตั้งใจเข้าไปหรือไม่ หากพบว่า URL ทำขึ้นมาจากตัวอักษรและตัวเลขแบบสุ่ม หรือดูน่าสงสัย อย่าใส่ข้อมูลใด ๆ เด็ดขาด

• ใช้การเข้ารหัส
ต้องมั่นใจว่าเมื่อคุณจำเป็นต้องให้ข้อมูลส่วนตัวจะต้องทำการเข้ารหัสทุกครั้ง ต้องตรวจสอบ URL ทุกครั้งให้ขึ้นต้นด้วย ‘https’นอกจากนี้ address bar และ browser’s status bar จะต้องแสดงสัญลักษณ์เล็ก ๆ ว่าล็อค

• ใช้คอมพิวเตอร์ของตัวเอง และเชื่อมต่อสัญญาณอินเทอร์เน็ตของตัวเอง

หลีกเลี่ยงการใช้คอมพิวเตอร์สาธารณะและสัญญาณไวไฟสาธารณะ เครื่องคอมพิมเตอร์สาธารณะอาจจะมีสปายแวร์อยู่จำนวนมาก ในสัญญาณไวไฟสาธารณะอาจมีความเสี่ยงในการถูกดักจับข้อมูลจากผู้ให้บริการเครือข่ายหรือจากอาชญากรไซเบอร์ และอาจถูกโจมตีด้วยไวรัสเครือข่าย

• ใช้รหัสผ่านที่คาดเดายากบนอุปกรณ์และบัญชีออนไลน์ของคุณ
ใช้รหัสผ่านความยาวตั้งแต่ 12 ตัวอักษรขึ้นไปในทุกที่ที่ทำได้ และใช้รหัสที่ต่างกัน ในแต่ละบริการหรือบัญชี

• กำจัดช่องโหว่ – ในระบบปฏิบัติการและแอปพลิเคชันของคุณด้วยการอัพเดท
เป็นการช่วยให้ลดช่องโหว่ของระบบปฏิบัติการและแอปพลิเคชัน ที่จะทำให้ถูกโจมตีจากโปรแกรมที่เป็นอันตรายได้

• ป้องกันอุปกรณ์ของคุณจากมัลแวร์และความเสี่ยงด้านความปลอดภัยบนอินเทอร์เน็ต
โซลูชั่นที่ป้องกันมัลแวร์สามารถป้องกันคุณจากไวรัสคอมพิวเตอร์ เวิร์ม โทรจันและไวรัสต่าง ๆ ในบางโซลูชั่นประกอบด้วยเทคโนโลยีพิเศษที่ให้ความปลอดภัยอีกระดับเมื่อคุณช้อปปิ้งออนไลน์และทำธุรกรรมทางธนาคาร

เกี่ยวกับ Kaspersky Security Network
Kaspersky Security Network (KSN) เป็นโครงสร้างพื้นฐานที่ซับซ้อนที่รวมเทคโนโลยีคลาวน์เบสเข้ากับสินค้าของ Kaspersky Lab ทั้งแบบส่วนตัวและองค์กร KSN ได้ทำการวิเคราะห์ข้อมูลด้านความปลอดภัยออนไลน์อย่างอัตโนมัติจากผู้ใช้นับหลายล้านคนทั่วโลก ด้วยการตรวจจับมัลแวร์อย่างรวดเร็วทั้งมัลแวร์ขั้นสูงและมัลแวร์ที่ไม่รู้จักมาก่อน กุญแจสู่ความสำเร็จของ KSN ก็คือการรวมกันของผู้เชี่ยวชาญด้านวิเคราะห์ข้อมูล ข้อมูลและการเรียนรู้อุปกรณ์ ระบบนี้ถือเป็นองค์ประกอบที่สำคัญที่สุดของ Kaspersky Labในการรักษาความปลอดภัยขั้นสูง
เกี่ยวกับ Kaspersky Lab
Kaspersky Lab เป็นบริษัทด้านความปลอดภัยบนอินเทอร์เน็ตระดับโลก ที่ดำเนินธุรกิจมากว่า 21 ปี ด้วยความเชี่ยวชาญด้านความปลอดภัยที่ได้พัฒนามาอย่างต่อเนื่อง จนปัจจุบันเปลี่ยนเป็นโซลูชั่นความปลอดภัยยุคใหม่ ที่ให้บริการในการป้องกันสำหรับธุรกิจ โครงสร้างพื้นฐาน รัฐบาลและลูกค้าทั่วโลก การให้บริการของบริษัทประกอบด้วยการป้องกันปลายทาง โซลูชั่นการป้องกันความปลอดภัยแบบพิเศษจำนวนมาก และบริการเพื่อป้องกันภัยคุกคามดิจิทัล ซึ่ง Kaspersky Lab ได้ป้องกันความปลอดภัยให้แก่ผู้ใช้กว่า 400 ล้านคน และอีกกว่า 270,000 องค์กร ที่ป้องกันความปลอดภัยให้กับทุกส่วนที่สำคัญสำหรับลูกค้า ศึกษาข้อมูลเพิ่มเติมได้ที่ www.kaspersky.com