แคสเปอร์สกี้ แลป สรุปตัวเลขเด่นด้านความปลอดภัย 2018

แคสเปอร์สกี้ แลป เปิดเผยว่า จากจำนวนข้อมูลไฟล์มุ่งร้ายใหม่ทั้งหมดที่ตรวจพบในปี 2018 มีจำนวนแรนซัมแวร์ที่เพิ่มขึ้นจากปีก่อน 43% มีจำนวนแบ็คดอร์เพิ่มขึ้น 44% และมีคอมพิวเตอร์จำนวน 1 ใน 3 หรือ 30.01% โดนโจมตีจากภัยคุกคามออนไลน์อย่างน้อย 1 ครั้งในปี 2018

ในเดือนมกราคม – ตุลาคม ปี 2018 การตรวจจับแรนซัมแวร์ (โทรจัน-แรนซัม) และแบ็คดอร์มีสัดส่วน 3.5% และ 3.7% จากจำนวนไฟล์มุ่งร้ายใหม่ทั้งหมด โดยมีจำนวนแรนซัมแวร์ที่เพิ่มขึ้นจากปีก่อน 43% (จำนวน 2,198,130 ปี 2017 เป็น 3,133,513 ปี 2018) มีจำนวนแบ็คดอร์เพิ่มขึ้น 44% (2,272,341 ปี 2017 เป็น 3,263,681 ปี 2018)

เทคโนโลยีตรวจจับของแคสเปอร์สกี้ แลป รับมือกับไฟล์มุ่งร้ายใหม่ๆ จำนวน 346,000 ไฟล์ในแต่ละวัน ตัวเลขจำนวนและประเภทของไฟล์ที่พบจากการตรวจจับในแต่ละวันจะเป็นตัวบ่งชี้ที่ดีในการวิเคราะห์ความสนใจของอาชญากรไซเบอร์ รวมถึงรูปแบบการสร้างและการแพร่กระจายมัลแวร์ ในปี 2011 เทคโนโลยีของแคสเปอร์สกี้ แลป ตรวจจับไฟล์มุ่งร้ายใหม่ได้ 70,000 ต่อวัน ในปี 2017 จำนวนไฟล์เพิ่มสูงขึ้นเป็น 360,000 ไฟล์หรือเพิ่มขึ้นเป็น 5 เท่า

นายอียาซสลาฟ ซาคอร์ชเชสกี้ หัวหน้าฝ่ายวิจัยแอนตี้มัลแวร์ ของแคสเปอร์สกี้ แลป กล่าวว่า “ในปี 2018 นี้ ตัวเลขการตรวจจับไฟล์มุ่งร้ายที่สร้างใหม่ในแต่ละวันมีจำนวนลดลงกว่าปีที่แล้ว ในทางหนึ่ง อาจบ่งชี้ได้ว่าอาชญากรไซเบอร์หันไปสนใจการใช้งานมัลแวร์เก่าที่รู้แล้วว่าทำงานมีประสิทธิภาพ แต่ในอีกทางหนึ่ง สัดส่วนของจำนวนแบ็คดอร์และโทรจันแรนซัมแสดงให้เห็นว่า ผู้ก่อเหตุพยายามหาวิธีใหม่ๆ ในการรุกล้ำเข้าดีไวซ์และหาเงินจากเหยื่อ การพัฒนาภัยคุกคามอย่าต่อเนื่องทำให้เราต้องตระหนักต่อภัยคุกคามต่างๆ ทั้งภัยที่มีอยู่แล้ว ภัยที่รู้จักและไม่รู้จัก นี่เป็นเหตุผลที่แคสเปอร์สกี้ แลป หมั่นปรับปรุงพัฒนาระบบการตรวจจับและการป้องกันในทุกๆ วัน เพื่อให้มั่นใจว่าลูกค้าของเราจะปลอดภัยจากภัยไซเบอร์”

ข้อมูลสถิติที่สำคัญอื่นๆ

โซลูชั่นของแคสเปอร์สกี้ แลป สามารถสกัดกั้นการโจมตีจากแหล่งออนไลน์จากทั่วโลกได้ถึง 1,876,998,691 ครั้ง
โซลูชั่นเว็บแอนตี้ไวรัสของแคสเปอร์สกี้ แลป สามารถตรวจจับอ็อพเจ็คอันตรายได้ 21,643,946 รายการ
คอมพิวเตอร์จำนวน 01% ประสบเหตุโจมตีด้วยมัลแวร์ออนไลน์อย่างน้อย 1 ครั้งในปีนี้

แคสเปอร์สกี้ แลป ขอแนะนำวิธีการปกป้องตนเองจากภัยไซเบอร์ดังนี้

ระมัดระวังและไม่เปิดไฟล์หรือไฟล์แนบที่น่าสงสัยที่ได้จากแหล่งไม่รู้ที่มา
ไม่ดาวน์โหลดและติดตั้งแอพพลิเคชั่นจากแหล่งที่เชื่อถือไม่ได้
ไม่คลิ้กลิ้งก์ที่ได้จากแหล่งไม่รู้ที่มา และไม่คลิ้กโฆษณาออนไลน์น่าสงสัยต่างๆ
ใช้พาสเวิร์ดที่มีความแข็งแกร่ง และเปลี่ยนพาสเวิร์ดอย่างสม่ำเสมอ
ติดตั้งการอัพเดทอย่างสม่ำเสมอ เพราะอัพเดทบางตัวมีการแก้ไขซ่อมแซมเรื่องความปลอดภัยที่สำคัญ
ไม่ควรกดยกเลิกระบบความปลอดภัย (disable) สำหรับซอฟต์แวร์ออฟฟิซและซอฟต์แวร์แอนตี้ไวรัส
ใช้โซลูชั่นเพื่อความปลอดภัยที่เหมาะสมกับประเภทของดีไวซ์และระบบที่ใช้งาน เช่น Kaspersky Internet Security และ Kaspersky Security Cloud

รายงานสถิตินี้เป็นส่วนหนึ่งของรายงาน Kaspersky Security Bulletin 2018 หากต้องการศึกษาเพิ่มเติมเกี่ยวกับการคาดการณ์ภัยคุกคามปี 2019 กรุณาติดตามที่นี่

Kaspersky Security Bulletin 2018. Threat Predictions for 2019