Kaspersky lab พัฒนาบริการรายงานภัยคุกคามขั้นสูง (API Intelligence Reporting Service) ด้วยการเพิ่มเติมโปรไฟล์ของผู้ก่อภัยคุกคามและเฟรมเวิร์ค MITRE ATT&CK

Kaspersky Lab ได้พัฒนาบริการรายงานภัยคุกคามขั้นสูง (APT Intelligence Reporting Service) ด้วยการเพิ่มข้อมูลเชิงบริบทที่เกี่ยวข้องกับผู้ก่อภัยคุกคามขั้นสูงและสามารถโยงเข้ากับโมเดล MITRE ATT&CK เพื่อค้นหาประวัติการถูกโจมตีก่อนหน้านี้ได้ การพัฒนาในครั้งนี้ยังช่วยให้ทีมปฏิบัติการด้านความปลอดภัยลงทะเบียนเป็นสมาชิกในบริการรายงานเอพีทีอันชาญฉลาด ที่ทำให้เข้าใจเป้าหมายของคู่ต่อสู้อย่างดีขึ้น ทั้งในด้านเทคนิคและประสิทธิภาพ ซึ่งวิธีนี้จะทำให้ทีมสามารถเชื่อมต่อกับเหตุการณ์ที่ผู้ก่อภัยคุกคาม เพื่อปรับปรุงความเข้าใจของแรงจูงใจที่อยู่เบื้องหลังการจู่โจมนั้น ๆ อีกทั้งทีมยังสามารถคาดการณ์ได้ว่านักจู่โจมจะทำอย่างไรในขั้นต่อไป เพื่อจะทำให้ป้องกันพวกเขาจากเหตุการณ์ต่าง ๆ ที่จะเกิดขึ้นในอนาคตได้

อาชญากรไซเบอร์กำลังพัฒนาเทคนิคที่ซับซ้อนในการโจรกรรมที่เป็นอันตรายต่อองค์กร จากรายงานการสำรวจด้านความปลอดภัยของ Kaspersky Lab เมื่อปี 2561 องค์กรต่าง ๆ ระบุว่าการโจรกรรมเป็นประเภทของความปลอดภัยทางไซเบอร์ที่ก่อให้เกิดความสูญเสียมากที่สุด ด้วยมูลค่าเฉลี่ยสูงกว่า 1.11 ล้านเหรียญสหรัฐ โดยการต่อสู้กับภัยคุกคามขั้นสูงนั้นไม่เพียงแต่จำเป็นต้องมีโซลูชั่นด้านความปลอดภัยที่เฉียบขาด แต่ยังต้องสามารถเข้าถึงระบบป้องกันภัยคุกคามอันชาญฉลาดที่ซับซ้อนและทันสมัยอยู่ตลอดเวลา เพื่อที่จะทำให้ทีมปฏิบัติการควบคุมและอยู่เหนือการโจมตีต่าง ๆ Kaspersky Lab จึงได้พัฒนาบริการรายงานภัยคุกคามขั้นสูง (APT) ที่ประกอบด้วยข้อมูลเชิงบริบทต่าง ๆ ของผู้ก่อการโจรกรรม รวมไปถึงกลวิธี เทคนิค แคมเปญ และกระบวนการต่าง ๆ ด้วย

การรายงานภัยคุกคามขั้นสูงของ Kaspersky Lab ยังสามารถแบ่งภาพรวมของภัยคุกคามขั้นสูงแต่ละประเภทได้ ซึ่งประกอบด้วยประเทศต้นกำเนิด นามแฝง รายการของเป้าหมายและเหยื่อก่อนหน้า รวมไปถึงเครื่องมือที่ใช้และรายละเอียดของแคมเปญที่ผ่านมา รายงานยังรวมถึงลิงค์ของแหล่งข้อมูลเพิ่มเติม ข้อมูลเฉพาะของ IoC และกฎ YARA ต่าง ๆ เพื่อที่จะช่วยให้องค์กรสามารถป้องกันการโจรกรรมเหล่านี้ได้

แคมเปญของภัยคุกคามขั้นสูงที่ค้นพบก่อนหน้านี้ได้เชื่อมไปยัง MITRE ATT&CK ซึ่งเป็นฐานความรู้ของกลวิธีและ

เทคนิคของฝ่ายตรงข้ามที่เข้าถึงได้ทั่วโลกภายใต้การสังเกตจากสถานการณ์ที่เกิดขึ้นจริงในโลก ผู้เชี่ยวชาญได้แบ่งการโจรกรรมออกเป็นส่วน ๆ เป็น PRE-ATT&CK และ ATT&CK ที่แสดงถึงกลวิธีและเทคนิคที่มีพลังในทุก ๆ ขั้นตอน เป็นการเสริมให้กลวิธีของ Kaspersky Lab ที่แบ่งเป้าหมายการโจมตีเข้าไปในเขตติดเชื้อ ชั้นตอนปลูกฝัง โครงสร้างพื้นฐาน เพื่อที่จะทำให้ผู้บริหารระดับสูงเข้าใจที่ในขั้นตอนที่สูงขึ้นของบริบทในภัยคุกคาม

“การแยกส่วนข้อมูลเกี่ยวกับการโจรกรรมไซเบอร์ขั้นสูง ทำให้ทีมปฏิบัติการด้านความปลอดภัยทำงานในการป้องกันยากขึ้น ดังนั้นทางเราถึงได้รวบรวม วิเคราะห์ และให้ข้อมูลที่ครอบคลุมเกี่ยวกับแคมเปญของภัยคุกคามขั้นสูง ร่วมด้วยการช่วยเหลือจาก MITRE ATT&CK เฟรมเวิร์ค ทำให้ตอนนี้เราสามารถแสดงแง่มุมเพิ่มเติมและบริบทของการปฏิบัติการเหล่านี้ ซึ่งทั้งหมดนี้จะทำให้องค์กรสามารถป้องกันและคาดการณ์ภัยคุกคามในอนาคตได้อย่างมีประสิทธิภาพ” มร. เซอร์จี มาร์ทชิงคยาน ผู้อำนวยการฝ่ายการตลาดผลิตภัณฑ์บีทูบี Kaspersky Lab
ศึกษาข้อมูลเพิ่มเติมเกี่ยวกับบริการรายงานภัยคุกคามขั้นสูง (APT Intelligence Reporting Service) ได้ที่ our official website.

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