# ภูมิศาสตร์ทางการเมืองและภูมิภาคเอเชียตะวันออกเฉียงชี้พลังภัยคุกคามในไตรมาสแรก ผู้โจมตีรายใหญ่ยังเงียบ

ไตรมาสแรกปี 2562 นักวิจัยของ Kaspersky Lab จับตาดูขอบเขตการปฏิบัติการของภัยคุกคามขั้นสูง โดยเกิดขึ้นในเอเชียตะวันออกเฉียงใต้เป็นหลัก เหตุที่มีภัยคุกคามมากขึ้นเป็นเพราะอิทธิพลของภูมิศาสตร์ทางการเมือง โดยเน้นที่ธุรกิจการแลกเปลี่ยนเงินคริปโตและสปายแวร์ที่โจมตีในเชิงการค้า รวมไปถึงโครงการซัพพลายเชนต่าง ๆ ซึ่งในรายงานสรุปภัยคุกคามรายไตรมาสของ Kaspersky Lab ได้ครอบคลุมถึงภัยคุกคามเหล่านี้รวมถึงแนวโน้มของภัยคุกคามอื่น ๆ อีกด้วย

รายงานสรุปภัยคุกคามรายไตรมาสของ Kaspersky Lab ได้รวบรวมจากการวิจัยภัยคุกคามอย่างชาญฉลาด รวมไปถึงจากแหล่งอื่น ๆ และให้ความสำคัญกับการพัฒนาหลัก ๆ ที่นักวิจัยเชื่อว่าทุกคนควรที่จะตระหนัก

ในไตรมาสแรกของปี 2562 นักวิจัยของ Kaspersky Lab จับตาดูการพัฒนาภัยคุกคามที่น่าสนใจจำนวนมาก การเผยแพร่ภัยคุกคามขั้นสูงรายงานการปฏิบัติงานในช่วง 3 เดือนของ ShadowHammer ซึ่งเป็นแคมเปญโจมตีขั้นสูงที่ใช้ซัพพลายเชนในการกระจายได้กว้างขวางอย่างน่าทึ่ง รวมกับเทคนิคที่ใช้ในการดำเนินการสำหรับการกำหนดเป้าหมายที่แม่นยำไปยังเหยื่อต่าง ๆ มากมาย

ภัยคุกคามขั้นสูงที่สำคัญในไตรมาสแรก ปี 2562 ประกอบด้วย

• องค์ประกอบของภูมิศาสตร์ทางการเมือง เป็นกุญแจสำคัญในการขับเคลื่อนของกิจกรรมของภัยคุกคามขั้นสูง ซึ่งจะเห็นได้อย่างชัดเจนว่าเมื่อมีการพัฒนาทางการเมืองก็จะมีกิจกรรมที่มุ่งร้าย

• ภูมิภาคเอเชียตะวันออกเฉียงใต้ยังคงเป็นพื้นที่ที่มีภัยคุกคามขั้นสูงจำนวนมากและรุนแรงติดอันดับโลก ที่มีภัยคุกคามขั้นสูงหลายกลุ่ม อีกทั้งมีสิ่งรบกวนจำนวนมาก และมีกิจกรรมโจมตีจากภัยคุกคามในภูมิภาคนี้มากกว่าภูมิภาคอื่น ๆ

• แม้ว่ากลุ่มรัสเซียยังคงอยู่ในระดับที่ลดลงเมื่อเทียบกับปีก่อน ๆ อาจเป็นเพราะองค์ประกอบของการจัดโครงสร้างภายใน แต่การแพร่กระจายของมัลแวร์ก็ยังคงมีอย่างต่อเนื่องจาก Sofacy และ Turla

• กลุ่มแฮกเกอร์ชาวจีน ยังคงทำกิจกรรมโจมตีอย่างต่อเนื่อง ทั้งแบบซับซ้อนสูงและต่ำขึ้นอยู่กับแคมเปญนั้น ๆ อาทิ เช่น กลุ่มที่ Kaspersky Lab รู้จักกันในนาม CactusPete เริ่มมีมาตั้งแต่ปี 2555 ซึ่งในไตรมาสแรกของปีนี้ได้ตรวจพบเครื่องมือใหม่ ๆ รวมไปถึงตัวดาวน์โหลดและแบค์ดอร์ที่ไม่เหมาะสมมากมาย อีกทั้งแพคเกจใหม่ที่ชื่อ VBScript zero-day ที่เป็นของกลุ่ม DarkHotel อีกด้วย

• ผู้ให้บริการของมัลแวร์ในเชิงพาณิชย์ ที่ส่งไปยังรัฐบาลและที่อื่น ๆ ดูเหมือนจะมีมากขึ้น นักวิจัยจับตาดู FinSpy รุ่นใหม่ ๆ รวมไปถึงการปฏิบัติการที่เรียกว่า LuckyMouse ที่คอยจัดการเมื่อเกิดข้อบกพร่องของเครื่องมือ HackingTeam

“เมื่อย้อนมองไปถึงสิ่งที่เกิดขึ้นในช่วงไตรมาสแรกที่ผ่านมาในปีนี้ ก็ยังคงประหลาดใจอยู่เสมอ ถึงแม้ว่าเรารู้สึกว่าสิ่งที่เกิดขึ้นไม่มีอะไรที่แหวกแนวออกไป โดยเราได้เปิดเผยขอบเขตพื้นที่ของภัยคุกคามที่น่าสนใจและวิวัฒนาการในส่วนต่าง ๆ ได้แก่ ในไตรมาสแรกมีการจู่โจมในรูปแบบซัพพลายเชนที่ซับซ้อน การโจมตีในการแลกเปลี่ยนเงินคริปโต และผู้ขับเคลื่อนภูมิศาสตร์ทางการเมือง เรารู้ว่าการตรวจสอบของเราอาจจะยังไม่ครอบคลุม ยังมีกิจกรรมการโจมตีในรูปแบบอื่นที่เรายังมองไม่เห็นหรือยังไม่เข้าใจ ดังนั้นในพื้นที่หรือภาคส่วนใดที่เราไม่ตรวจพบภัยคุกคาม ไม่ได้หมายความว่ามันจะไม่มีในอนาคต การป้องกันภัยคุกคามทั้งในแบบที่รู้หรือไม่รู้ก็ตามยังคงมีความจำเป็นอย่างยิ่งสำหรับทุกคน” มร. วินเซนต์ ดิแอซ ผู้อำนวยการใหญ่ด้านความปลอดภัย ทีมวิจัยและวิเคราะห์ระดับโลก Kaspersky Lab

รายงานสรุปแนวโน้มภัยคุกคามของไตรมาสแรกของ Kaspersky Lab บริการให้สำหรับสมาชิกเท่านั้น ซึ่งแนบมากับ ข้อมูล IOC และ YARA rules ที่จะช่วยในการตรวจจับและล่ามัลแวร์ สำหรับข้อมูลเพิ่มเติมติดต่อได้ที่ intelreports@kaspersky.com

เพื่อหลีกเลี่ยงจากการตกเป็นเหยื่อของการโจมตีของภัยคุกคาม นักวิจัยของ Kaspersky Lab แนะนำให้ปฏิบัติตามดังนี้

• จัดหาระบบจัดการภัยคุกคามที่ชาญฉลาดให้กับทีมรักษาความปลอดภัยของคุณ เพื่อจะได้รู้ทัน และอัพเดทเครื่องมือ เทคนิค และวิธีการต่าง ๆ ของอาชญากรที่จ้องโจมตีอยู่ เพื่อที่จะเตรียมรับมือได้

• สำหรับระดับการป้องกัน ตรวจสอบ และแก้ไขสถานการณ์อย่างทันท่วงที ใช้โซลูชั่นป้องกันภัยคุกคามอย่าง Kaspersky Endpoint Detection and Response

• นอกจากการนำชุดป้องกันภัยคุกคามไปใช้แล้ว จำเป็นต้องมีชุดการป้องกันภัยคุกคามขั้นสูงในเครือข่าย ตั้งแต่ในระดับเริ่มต้น อย่าง Kaspersky Anti Targeted Attack Platform

• เนื่องจากภัยคุกคามเริ่มโจมตีด้วย ฟิชชิ่ง หรือเทคนิคอื่น ๆ ดังนั้นจำเป็นต้องมีการจัดอบรมให้ทีมตระหนักและเข้าใจ โดยมีทั้งการอบรมและการเพิ่มทักษะ เช่นแพลตฟอร์ม Kaspersky Automated Security Awareness Platform

รายงานแนวโน้มภัยคุกคาม ไตรมาสแรก ปี 2562 มีใน Securelist แล้วตอนนี้

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