แคสเปอร์สกี้ แลป คาดการณ์ภัยคุกคาม 2019: ผู้ร้ายไซเบอร์จะงัดอาวุธหนักพร้อมกลยุทธ์ใหม่ หวังโจมตีทำลายล้าง

จากรายงาน “Targeted Threat Predictions for 2019” ของแคสเปอร์สกี้ แลป ระบุว่า ในปี 2019 นี้ เราจะได้เห็นวงการ APT แบ่งเป็นสองกลุ่ม กลุ่มแรกคือผู้ร้ายหน้าใหม่ที่ไม่มีประสบการณ์แต่กระเหี้ยนกระหือรือที่จะเล่นเกมร้ายไซเบอร์ และกลุ่มผู้ร้ายเก่าหน้าเดิมที่มีทักษะขั้นสูงและมีแหล่งทรัพยากรแข็งแกร่ง โดยกลุ่มผู้ร้ายเดิมนี้จะปฏิบัติการท้าทายองค์กรธุรกิจครั้งใหญ่ ด้วยมีประสบการณ์สูงและมีเทคนิคใหม่ๆ ที่ซับซ้อนมากขึ้น ทำให้ยากในการค้นหาและกำจัดยิ่งขึ้นไปอีก

รายงานคาดการณ์ประจำปีฉบับนี้ ทีมวิเคราะห์และวิจัยระดับโลกของแคสเปอร์สกี้ แลป (Global Research and Analysis Team หรือ ทีม GReAT) เป็นผู้คาดการณ์ภัยคุกคามแบบระบุเป้าโจมตี โดยวิเคราะห์จากข้อมูลความรู้ความเชี่ยวชาญที่สะสมจากปีที่ผ่านมา รายงานนี้จะช่วยให้ผู้เกี่ยวข้องสามารถเข้าใจและเตรียมรับมือความท้าทายด้านความปลอดภัยไซเบอร์ที่อาจจะประสบพบเจอได้ในปีหน้า

คาดว่าจะไม่มีเหตุการณ์โจมตี APT ครั้งใหญ่
คาดการณ์ว่า ปีหน้าวงการความปลอดภัยไซเบอร์จะได้เห็นปฏิบัติการซับซ้อนที่ได้รับการสนับสนุนจากรัฐบาลหลายเหตุการณ์อย่างต่อเนื่อง แต่ผู้โจมตีสร้างภัยคุกคามก็จะหลบซ่อนไม่ทำตัวโดดเด่น เพื่อหลบเลี่ยงการตรวจจับและถูกเปิดโปงต่อสาธารณะ และด้วยทรัพยากรที่มี ก็ยังสามารถขยายเครื่องมือเครื่องไม้และการดำเนินการต่างๆ ได้ ทำให้การตรวจจับภัยคุกคามนั้นยากขึ้นมาก

หนึ่งในเหตุการณ์ที่น่าจะเกิดขึ้นก็คือ การใช้ทูลที่เจาะจงตรงไปยังแกนหลักของเหยื่อเป้าหมายที่เลือกไว้โดยเฉพาะ นั่นคือการแทรกแซงฮาร์ดแวร์ของเครือข่าย กลยุทธ์ใหม่นี้จะทำให้ผู้โจมตีสามารถแทรกแซงในลักษณะบ็อตเน็ตได้ หรืออาจจะแอบโจมตีเฉพาะเป้าหมายที่เลือกไว้ก็ได้

การคาดการณ์ที่สำคัญอื่นๆ ในปี 2019 มีดังนี้
• การโจมตีซัพพลายเชนยังมีอยู่ – การโจมตีซัพพลายเชนเป็นเรื่องที่น่ากังวลมากที่สุดเรื่องหนึ่ง ซึ่งผู้ร้ายไซเบอร์ได้ดำเนินการสำเร็จอย่างดีในช่วง 2 ปีที่ผ่านมา ทำให้หลายองค์กรเริ่มทบทวนจำนวนโพรไวเดอร์ที่ต้องทำงานร่วมกันและเริ่มพิจารณาเรื่องความปลอดภัยของโพรไวเดอร์ ในปีหน้า จะพบเหตุการณ์การโจมตีที่มีประสิทธิภาพ

• ยังมีโมบายมัลแวร์แน่นอน – ผู้ร้ายไซเบอร์จำนวนมากมีโมบายคอมโพเน้นต์รวมอยู่ในแคมเปญของตัวเอง เพื่อใช้เพิ่มจำนวนเหยื่อที่เป็นไปได้ คาดว่าจะไม่พบการแพร่กระจายโมบายมัลแวร์แบบเจาะจงเป้าหมายครั้งใหญ่ แต่จะได้เห็นกิจกรรมการโจมตีและวิธีการโจมตีขั้นสูงแนวใหม่ๆ เพื่อเข้าแอคเซสดีไวซ์ของเหยื่ออย่างแน่นอน
• ไอโอทีบ็อตเน็ตจะโตต่อเนื่องไม่หยุด – ผู้เชี่ยวชาญในวงการได้ออกมาเตือนภัยบ็อตเน็ตของอินเทอร์เน็ตออฟธิงส์ซ้ำๆ ทุกปีเพื่อความไม่ประมาท และในปีหน้านี้บ็อตเน็ตประเภทนี้ก็จะเพิ่มจำนวนและมีประสิทธิภาพมากยิ่งขึ้นเมื่อถูกใช้งานโดยผู้ไม่หวังดีอย่างผู้ร้ายไซเบอร์
• การโจมตีสเปียร์ฟิชชิ่งจะสำคัญมากขึ้นในอนาคตอันใกล้ – ข้อมูลที่ได้จากการโจมตีโซเชียลมีเดียรายใหญ่อย่าง เช่น Facebook, Instagram, LinkedIn และ Twitter ตอนนี้มีวางขายในตลาดมืดแล้ว ทั้งนี้ เหตุการณ์ข้อมูลรั่วไหลขนาดใหญ่ล่าสุดจากแต่ละแพลตฟอร์มอาจช่วยให้ผู้โจมตีได้พัฒนาปรับปรุงการแพร่กระจายได้ด้วย
• ผู้ร้าย APT หน้าใหม่จะขอมีบทบาท – คาดว่าผู้โจมตีขั้นสูงจะเก็บเนื้อเก็บตัวหายไปจากเรดาร์ และจะมีผู้ร้ายหน้าใหม่ปรากฏตัวขึ้น ด้วยทูลที่มีประสิทธิภาพสูงนับร้อยๆ ทูล เอ็กซ์พลอต์ที่มีจุดอ่อน และเฟรมเวิร์กต่างๆ ที่เปิดกว้างให้ทุกคนได้ใช้งาน ทำให้ปราการป้องกันด้านความปลอดภัยไซเบอร์นั้นเปราะบางลงได้อีก คาดว่าภูมิภาคที่เป็นเป้าหมายการโจมตีอย่างแพร่หลายนี้คือ เอเชียตะวันออกเฉียงใต้และตะวันออกกลาง
• การโต้ตอบของสาธารณชนจะเปลี่ยนรูปแบบวงการความปลอดภัยไซเบอร์ – การสืบสวนเหตุการณ์โจมตีชื่อดังอย่างการโจมตีบริษัทโซนี่และคณะกรรมการแห่งชาติพรรคเดโมแครต สหรัฐอเมริกา ได้ยกระดับความยุติธรรมและการเปิดเผยต่อสาธารณะเรื่องการคุกคามไซเบอร์ไปอีกขั้น การเปิดโปงและความโกรธขึ้งของสาธารณชน จะก่อให้เกิดกระแสความคิดเห็นไปจนถึงการตอบโต้เพื่อให้ได้ผลลัพธ์จริงจังอย่างมีชั้นเชิงทั่วโลก

นายวิเซนเต้ ดิแอซ นักวิจัยด้านความปลอดภัยของแคสเปอร์สกี้ แลป กล่าวว่า “การโจมตีในปี 2018 ทำให้เกิดกระบวนทัศน์รูปแบบใหม่ คือสาธารณชนตระหนักรู้เรื่องภัยคุกคามไซเบอร์เพิ่มมากขึ้น การสืบสวนของผู้เชี่ยวชาญยังได้ชี้จุดสำคัญของปฏิบัติการโจมตีไซเบอร์ครั้งใหญ่ๆ และเป็นข่าวดังไปทั่วโลก ซึ่งจะทำให้เกิดการเปลี่ยนแปลงรูปแบบของโลกไซเบอร์ได้ เนื่องจากผู้ร้ายขั้นสูงที่มีความซับซ้อนจะเปลี่ยนเป็นหลบซ่อนตัวเงียบๆ เพื่อให้การโจมตีครั้งต่อไปประสบความสำเร็จมากขึ้น การเปลี่ยนแปลงนี้จะทำให้การตรวจสอบค้นหาปฏิบัติการร้ายเป็นไปอย่างยากลำบากมากยิ่งขึ้น แต่ก็จะทำให้เกิดการพัฒนาปรับปรุงวิธีการตรวจจับผู้ร้ายไซเบอร์ไปอีกขั้นอย่างแน่นอน”

รายงานการคาดการณ์นี้พัฒนาขึ้นจากข้อมูล Threat Intelligence Services ของแคสเปอร์สกี้ แลป จากทั่วโลก โดยล่าสุด แคสเปอร์สกี้ แลป ได้รับการคัดเลือกเป็นผู้ดำเนินการที่มีความแข็งแกร่ง หรือ “Strong Performer” ด้าน Threat Intelligence จากสถาบันวิจัยฟอร์เรสเตอร์

ท่านสามารถอ่านรายงาน Kaspersky Lab Threat Predictions for 2019 ฉบับเต็มได้ที่

Kaspersky Security Bulletin 2018. Threat Predictions for 2019