A10 Networks เปิดเผยงานวิจัยภัยคุกคาม พร้อมตรวจพบ DDoS มากกว่า 15 ล้านรายการ

จากมีรายงานว่าในช่วงเวลาที่เกิดโรคระบาด การโจมตีทางไซเบอร์ก็เพิ่มขึ้นอย่างรวดเร็ว ไม่ว่าจะเป็น มัลแวร์ แรนซัมแวร์ และการโจมตีแบบ DDoS ผู้คุกคามไม่เพียงพยายามขัดขวางการใช้บริการในชีวิตประจำวันที่ผู้คนต้องใช้งาน เช่น การดูแลสุขภาพ การศึกษา และการเงิน แต่ยังรวมถึงโครงสร้างพื้นฐานที่สำคัญ ไม่ว่าจะเป็น ซัพพลายเชนด้านอาหาร สาธารณูปโภค และ หน่วยงานของภาครัฐอีกด้วย ในขณะเดียวกัน ก็มีอาวุธทางไซเบอร์ที่สามารถใช้เพื่อทำการโจมตีเหล่านี้เพิ่มขึ้นเป็นอันมาก

ช่วงครึ่งหลังของปี พ.ศ. 2564 ทีมวิจัยด้านความปลอดภัยของ A10 Networks ได้พบว่ามีอาวุธไซเบอร์ที่ใช้โจมตีแบบ DDoS เกิดขึ้นมากกว่า 15.4 ล้านรายการ นอกจากนี้ข่าวกรองด้านภัยคุกคามของ A10 Networks ให้รายละเอียดเกี่ยวกับการใช้การโจมตีแบบ DDoS ว่า เกิดขึ้นเพื่อขัดขวางโครงสร้างพื้นฐานและการสื่อสารในยูเครนเมื่อเดือนกุมภาพันธ์ พ.ศ 2565 ที่ผ่านมา ซึ่งเป็นช่วงเดียวกันกับที่รัสเซียเปิดการโจมตีภาคพื้นดิน

ทีมวิจัยข่าวกรองภัยคุกคามของ A10 ได้ติดตามความคืบหน้าที่สำคัญทั้งในด้านขอบเขตและความรุนแรงของอาชญากรรมทางอินเทอร์เน็ต และระบุว่า:

- อาวุธการโจมตีแบบ DDoS มีจำนวนเพิ่มขึ้น: ทั้ง 15.4 ล้านรายการ ได้ถูกติดตามโดยทีมวิจัยความปลอดภัยของ A10 แล้ว
- อาวุธสำหรับโจมตีที่ขยายขีดความสามารถด้านการแอบแฝงซ่อนเร้น มีจำนวนเพิ่มขึ้นมากกว่า 100 เปอร์เซ็นต์ เมื่อเทียบปีต่อปี ซึ่งรวมถึง Apple Remote Desktop (ARD) ซึ่งถูกใช้ในช่วงที่เกิดความขัดแย้งระหว่างรัสเซียกับยูเครน
- ผู้โจมตีได้ใช้ประโยชน์จากช่องโหว่ Log4j ที่รู้จักกันดีในขณะนี้ โดยเครื่องมือค้นหาช่องโหว่ Log4j จำนวนมากกว่า 75 เปอร์เซ็นต์ มีต้นกำเนิดอยู่ในรัสเซีย

ข้อมูลเหล่านี้และแนวโน้มอื่น ๆ ถูกรวบรวมอยู่ในรายงานภัยคุกคาม “2022 A10 Networks DDoS Threat Report” รวมถึงที่มาของกิจกรรมการโจมตีแบบ DDoS การเติบโตของอาวุธ DDoS, คอมพิวเตอร์, เซิร์ฟเวอร์, อุปกรณ์ IoT ที่อาจใช้ในการโจมตีแบบ DDoS และบ็อตเน็ต รายงานนี้ยังรวมถึงบทบาทของมัลแวร์ในการโจมตี กระจายของอาวุธ DDoS และขั้นตอนที่องค์กรสามารถดำเนินการเพื่อป้องกันกิจกรรมดังกล่าวได้

องค์กรต่างๆ ต้องดำเนินการทันที โดยใช้หลักการ Zero Trust

จากข้อมูลเมื่อวันที่ 21 มีนาคม 2022 ที่ผ่านมาหน่วยงาน Biden-Harris Administration ได้ออกคำแนะนำให้องค์กรต่าง ๆ ของสหรัฐอเมริกาต้องดำเนินการอย่างรวดเร็วเพื่อป้องกันการโจมตีทางไซเบอร์และสงครามไซเบอร์ที่รัฐสนับสนุน อันเนื่องมาจากความขัดแย้งระหว่างรัสเซียกับยูเครนที่กำลังดำเนินอยู่

ทั้งนี้คำแนะนำดังกล่าวมุ่งเป้าไปที่องค์กรต่างๆ ในสหรัฐอเมริกา ขณะเดียวกันก็ชี้แจงถึงความจำเป็นเร่งด่วนที่องค์กรต่างๆ ทั่วโลกจะต้องประเมินจุดยืนด้านความปลอดภัยของตนอีกครั้ง การใช้หลักการ Zero Trust ไม่เพียงช่วยปกป้องเครือข่าย แต่ยังช่วยให้แน่ใจว่าเครือข่ายจะไม่ถูกนำไปใช้เพื่อเป็นจุดเริ่มการโจมตี โซลูชันด้านความปลอดภัยสำหรับการป้องกันการโจมตีแบบ DDoS, การตรวจสอบ TLS/SSL ในการรับส่งข้อมูลแบบเข้ารหัส และความสามารถด้านการรักษาความปลอดภัยใน การจัดส่งแอปพลิเคชันของ A10 สามารถกำหนดนโยบาย Zero Trust ที่อิงตามอัตลักษณ์บุคคลและตามบริบทเพื่อบังคับใช้ในการเข้าใช้งาน

"เหตุการณ์ล่าสุดเน้นย้ำถึงผลกระทบที่ร้ายแรงจากการโจมตีทางไซเบอร์ต่อรัฐบาลและธุรกิจทั่วโลก เครือข่าย A10 ติดตามต้นกำเนิดของกิจกรรมอาวุธการโจมตีแบบ DDoS นอกเหนือจากปัจจัยการโจมตีอื่น ๆ เพื่อติดอาวุธให้กับลูกค้าด้วยข่าวกรองภัยคุกคามที่เป็นประโยชน์ นี่เป็นองค์ประกอบที่สำคัญของเฟรมเวิร์ก Zero Trust เพื่อช่วยให้องค์กรสามารถคาดการณ์และลดการโจมตีทางไซเบอร์ได้ดียิ่งขึ้น และยังช่วยให้มั่นใจว่าเครือข่ายไม่ได้ถูกอาวุธโดยไม่ได้ตั้งใจ" Mr.Dhrupad Trivedi ประธานและซีอีโอของ A10 Networks กล่าว

อย่างไรก็ตามเพื่อเป็นเครื่องพิสูจน์ถึงนวัตกรรมเทคโนโลยีของ A10 เมื่อเร็วๆ นี้ Frost & Sullivan ได้ประเมินโซลูชันการป้องกัน DDoS ของ A10 ร่วมกับผู้จำหน่ายรายอื่นหลายราย และได้มอบ “รางวัลผู้นำคุณค่าสำหรับลูกค้าของ Frost & Sullivan ประจำปี 2021 ในด้านการลดความเสี่ยง DDoS ระดับสากล ด้านความเป็นเลิศในแนวทางปฏิบัติที่ดีที่สุด” ให้กับ A10

นอกจากนี้ เพื่อสนับสนุนความต้องการความปลอดภัยทางไซเบอร์ของลูกค้าและสนับสนุนโซลูชันระดับโลกสำหรับการป้องกันภัยคุกคามทางไซเบอร์ ทาง A10 จึงได้เข้าร่วมกับ Microsoft Intelligent Security Association (MISA) ซึ่งเป็นระบบนิเวศของผู้จำหน่ายซอฟต์แวร์อิสระและผู้ให้บริการด้านความปลอดภัยที่มีการจัดการที่ผสานรวมโซลูชันของพวกเขา เพื่อป้องกันโลกของภัยคุกคามที่เพิ่มขึ้นได้ดียิ่งขึ้น