imperva
a Thales company

รายงานภูมิทัศน์ภัยคุกคามจาก DDoS ปี 2024 ของ Imperva

imperva
a Thales company

รายงานภูมิทัศน์ภัยคุกคามจากDDoSปี 2024 ของ Imperva

สารบัญ

รายงานภูมิทัศน์ภัยคุกคามจาก DDoS

รายงานภูมิทัศน์ภัยคุกคามทางไซเบอร์จาก DDoS ปี 2024 ของ Imperva จะมีข้อมูลเหตุการณ์การโจมตีแบบ Distributed Denial of Service (DDoS) ในช่วงครึ่งแรกของปี 2024 โดยจะให้ข้อมูลเชิงลึกเกี่ยวกับเหตุการณ์ DDoS ที่โดดเด่นที่สุดของปี และให้คำแนะนำสำหรับปีหน้า

การโจมตี DDoS เกิดขึ้นมานานแล้วและยังไม่มีทีท่าว่าจะหมดไป อาชญากรไซเบอร์มีเจตนาทำให้ระบบหยุดชะงัด ไม่ว่าจะด้วยเหตุผลทางการเมืองหรือเพียงแค่ในนามของนักเคลื่อนไหวทางการเมืองบนโลกไซเบอร์ทั่วไป โดยมักจะใช้การโจมตีประเภทนี้เป็นตัวเลือกการดำเนินการครั้งแรก

สิ่งที่เห็นได้ชัดก็คือจำนวนการโจมตีเหล่านี้กำลังเพิ่มขึ้นเรื่อย ๆ แรงขับเคลื่อนนั้นมาจากการที่เครื่องมือ DDoS พร้อมใช้งานอย่างสะดวกง่ายดายมากขึ้น ซึ่งแม้แต่บุคคลที่มีความเชี่ยวชาญทางเทคนิคไม่มากก็สามารถดำเนินการโจมตีที่ส่งผลรุนแรงได้ การเปลี่ยนแปลงสู่ระบบอัตโนมัติในเครื่องมือเหล่านี้ช่วยลดอุปสรรคในการเข้าสู่ระบบ ทำให้อาชญากรไซเบอร์สามารถโจมตี DDoS ได้หลากหลายรูปแบบมากขึ้น

ความตึงเครียดทางการเมืองยังมีส่วนทำให้การโจมตี DDoS เกิดขึ้นบ่อยครั้ง เนื่องจากรัฐและนักเคลื่อนไหวใช้วิธีการเหล่านี้เพื่อสร้างถ้อยแถลงทางการเมืองหรือส่งสัญญาณถึงการกระทำที่อาจเกิดขึ้นในอนาคต ดังนั้น การทำความเข้าใจแรงจูงใจและวิธีการเบื้องหลังการโจมตี DDoS จึงเป็นสิ่งสำคัญสำหรับการพัฒนากลยุทธ์การป้องกันที่มีประสิทธิภาพ

รายงานดังกล่าวใช้ประโยชน์จากข้อมูลที่ได้รับจาก Imperva Threat Research โดยอิงตามข้อมูลจากแอปพลิเคชันและการโจมตี DDoS ในระดับเครือข่ายที่เราช่วยบรรเทาให้น้อยลง นอกจากนี้ รายงานยังให้ข้อสังเกตเพิ่มเติมตามกิจกรรม DDoS ในวงกว้างของทั่วโลกตลอดทั้งปี

ข้อมูลเชิงลึกและคำแนะนำที่ให้ไว้ในรายงานนี้เป็นสิ่งสำคัญสำหรับองค์กรที่มีเป้าหมายที่จะยกระดับสถานะความปลอดภัยทางไซเบอร์ของตนเพื่อรับมือกับภูมิทัศน์ที่ภัยคุกคามด้าน DDoS กำลังรุดหน้าอย่างรวดเร็ว

การโจมตี DDoS คืออะไร

04

การโจมตีแบบ Distributed Denial of Service (DDoS) แบ่งออกได้เป็นประเภทหลัก ได้แก่ การโจมตีตามปริมาณ การโจมตีโปรโตคอล และการโจมตีแอปพลิเคชันเลเยอร์

นับตั้งแต่เริ่มมีการโจมตีในช่วงต้นทศวรรษที่ 1990 แรงจูงใจเบื้องหลังการโจมตี DDoS ได้ก่อตัวขึ้นจากการกลั่นแกล้งระรานทางไซเบอร์และการแก้แค้นไปจนถึงการเคลื่อนไหวทางการเมืองบนโลกไซเบอร์ การทำสงครามทางไซเบอร์ และการขู่กรรโชก/Ransom DDoS (RDoS) ในขณะเดียวกัน วิธีการที่ใช้ในการโจมตี DDoS ก็มีความก้าวหน้ามากขึ้น

การโจมตี DDoS เกิดขึ้นจากอุปกรณ์ที่เชื่อมต่อหลายเครื่องและกระจายอยู่ทั่วเครือข่ายอินเทอร์เน็ต ทำให้การบรรเทาปัญหาทำได้ยาก เนื่องจากจำนวนอุปกรณ์ที่เกี่ยวข้อง การโจมตี DDoS ขนาดใหญ่เหล่านี้มักเกี่ยวข้องกับบอทเน็ต ซึ่งเป็นเครือข่ายของอุปกรณ์ที่ถูกบุกรุก ซึ่งถูกควบคุมจากระยะไกลจากศูนย์ควบคุมและสั่งการ (C&C)

สามารถดูประเภทการโจมตี DDoS แบบละเอียดและวิธีการบรรเทาปัญหาได้ที่นี่

ผู้โจมตีใช้การโจมตี DDoS เพื่อวัตถุประสงค์หลายอย่าง รวมถึงการเคลื่อนไหวทางการเมืองบนโลกไซเบอร์ และเจตนาที่เป็นอันตรายอื่นๆ

ข้อมูลสรุปสำหรับผู้บริหาร

05

จุดเด่นในรายงาน

111%

การเพิ่มขึ้นของการโจมตี DDoS ที่ Imperva ช่วยรับมือ ในช่วงครึ่งแรกของปี 2024 Imperva ประสบความสำเร็จในการลดการโจมตี DDoS ได้เพิ่มขึ้น 111% เมื่อเทียบกับช่วงเดียวกันของปีที่แล้ว โดยเน้นถึงความจำเป็นในการใช้มาตรการรักษาความปลอดภัยที่มีประสิทธิภาพ

4.7 ล้าน RPS

การโจมตี DDoS ของแอปพลิเคชันเลเยอร์จำนวน 4.7 ล้าน RPS: การโจมตีที่เด่นที่สุดในช่วงครึ่งแรกของปี 2024 คือการโจมตี DDoS ต่อแอปพลิเคชันเลเยอร์ในเดือนกุมภาพันธ์ โดยทำสถิติที่ 4.7 ล้านคำขอต่อวินาที (RPS)

215%

การโจมตี DNS เพิ่มขึ้น 215%: การโจมตี DNS เพิ่มขึ้น 215% เมื่อเปรียบเทียบ H1 2024 กับระยะเวลาเดียวกันในปี 2023

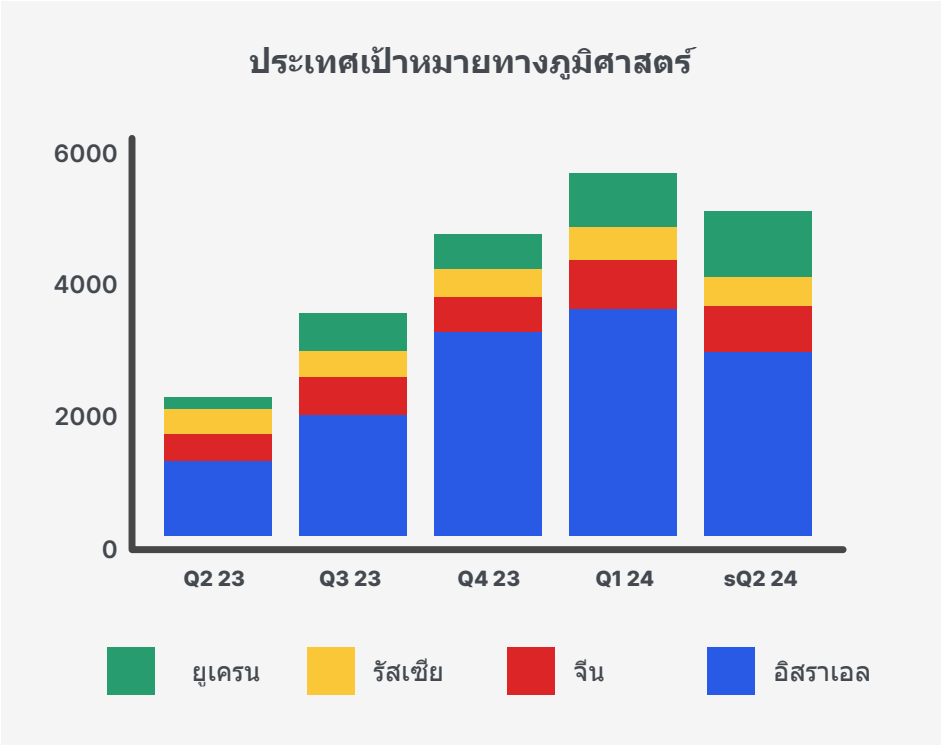
483%

การเพิ่มขึ้นของขนาดของการโจมตี DNS Amplification ในครึ่งหลังของปี 2023 ขนาดเฉลี่ยของการโจมตีแบบ DNS Amplification เพิ่มขึ้น 483% เมื่อเทียบกับครึ่งแรกของปี

ความตึงเครียดทางภูมิศาสตร์ที่ขับเคลื่อนจำนวนการโจมตี DDoS

ความตึงเครียดทางภูมิรัฐศาสตร์ทำให้การโจมตี DDoS เพิ่มจำนวนมากขึ้นอย่างมีนัยสำคัญในช่วงปีที่ผ่านมา พื้นที่หลักที่ได้รับผลกระทบ ได้แก่:

ความไม่สงบในตะวันออกกลาง	**118%** การโจมตีอิสราเอลเพิ่มขึ้น	+118%
ความขัดแย้งระหว่างรัสเซียและยูเครน	**519%** การโจมตียูเครนเพิ่มขึ้น	+519%
การแข่งขันด้านการรักษาความปลอดภัยทางไซเบอร์	**84%** การโจมตีในจีนเพิ่มขึ้น	+84%



89%

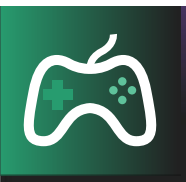
การเพิ่มขึ้นของการโจมตี DDoS ในการแข่งขันกีฬา
การโจมตี DDoS ที่มุ่งเป้าไปที่อุตสาหกรรมที่เกี่ยวข้องกับการแข่งขันกีฬารายสำคัญเพิ่มขึ้นถึง 89% ซึ่งแสดงให้เห็นว่ากิจกรรมสำคัญมูลค่าสูงย่อมดึงดูดอาชญากรไซเบอร์ที่พยายามขัดขวางการดำเนินงานและประชาสัมพันธ์

548%

การเพิ่มขึ้นของการโจมตีระบบโทรคมนาคมและ ISP
ภาคธุรกิจโทรคมนาคมและ ISP ประสบกับการโจมตี DDoS เพิ่มขึ้น 548% ซึ่งสะท้อนถึงบทบาทที่สำคัญในการดูแลรักษาความมั่นคงของการเชื่อมต่ออินเทอร์เน็ตและเดิมพันที่สูงในการขัดขวางบริการของพวกเขา

236%

การเพิ่มขึ้นของการโจมตีเป้าหมายที่เป็นธุรกิจการดูแลสุขภาพ
การโจมตีองค์กรด้านการดูแลสุขภาพเพิ่มขึ้น 236% ซึ่งชี้ให้เห็นได้ชัดถึงช่องโหว่ของภาคธุรกิจนี้ และผลกระทบที่อาจก่อให้เกิดความเสียหายร้ายแรงต่อบริการการดูแลสุขภาพที่สำคัญและข้อมูลผู้ป่วย



208%

การเพิ่มขึ้นของการโจมตีอุตสาหกรรมเกม การโจมตีอุตสาหกรรมเกม รวมถึงแพลตฟอร์มการพนันออนไลน์เพิ่มขึ้น 208% ซึ่งสะท้อนถึงเป้าหมายที่มีมูลค่าสูงและความอ่อนไหวต่อการหยุดชะงักของภาคธุรกิจที่อาจส่งผลกระทบต่อประสบการณ์การเล่นเกมและธุรกรรมทางการเงิน

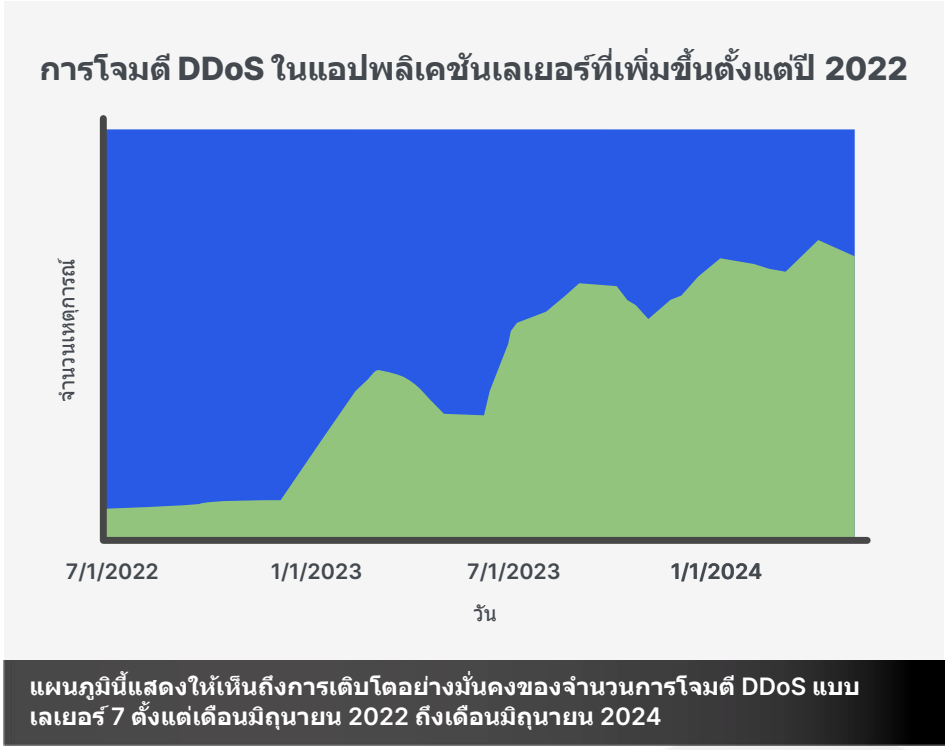
การโจมตีแบบ DDoS เติบโตขึ้นทั้งในแง่ของจำนวนและขนาด

07

การโจมตีแบบ DDoS เติบโตขึ้นในแง่ของจำนวน

จำนวนรวมของการโจมตี DDoS ที่บันทึกไว้เพิ่มขึ้น 111% เมื่อเทียบกับปีก่อนหน้า ตัวเลขที่เพิ่มขึ้นอย่างเห็นได้ชัดนี้ ช่วยให้เราตระหนักถึงภัยคุกคามที่เพิ่มมากขึ้นและความสำคัญที่เพิ่มขึ้นของการมีกลยุทธ์การบรรเทา DDoS ที่แข็งแกร่ง

การโจมตีแอปพลิเคชันเลเยอร์เพิ่มขึ้น 110% เมื่อเทียบปีต่อปี โดยมีการรับมือครั้งใหญ่ที่สุดถึง 4.7 ล้าน RPS ในวันที่ 24 กุมภาพันธ์



แผนภูมินี้แสดงให้เห็นถึงการเติบโตอย่างมั่นคงของจำนวนการโจมตี DDoS แบบเลเยอร์ 7 ตั้งแต่เดือนมิถุนายน 2022 ถึงเดือนมิถุนายน 2024

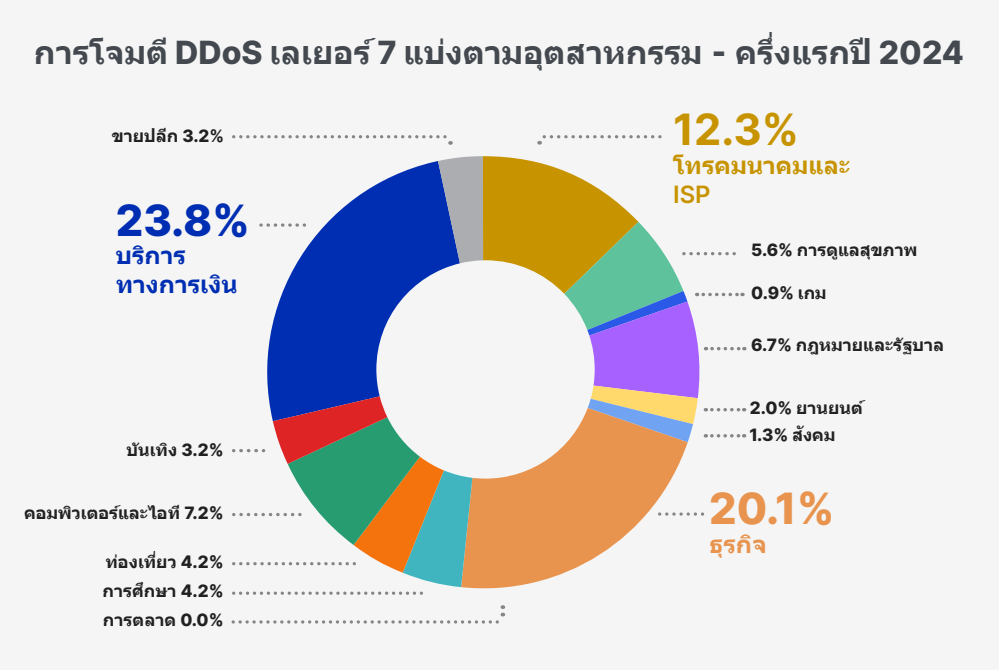
การโจมตี DDoS เติบโตขึ้นในแง่ของขนาด

การโจมตี DDoS ได้เพิ่มขึ้นอย่างมีนัยสำคัญในแง่ของขนาด เหตุการณ์สำคัญ ได้แก่:

- กุมภาพันธ์ **2024:** การโจมตี DDoS แบบเลเยอร์ 7 ครั้งสำคัญที่สุดที่มุ่งเป้าไปที่เว็บไซต์เกมของอินโดนีเซียที่มี 4.7 ล้าน RPS จาก 1,700 IP ในแคนาดา อินเดีย และสหรัฐอเมริกา
- **ในเดือนมีนาคม 2024** เราช่วยลดการโจมตีขนาดใหญ่ที่ไม่ค่อยเกิดขึ้นกับเว็บไซต์ค้าปลีกออนไลน์ในโรมาเนียที่ประเมินค่าได้ 4M RPS ซึ่งเป็นการเพิ่มขึ้น 2,000% จากประวัติก่อนหน้าสำหรับการโจมตีในประเทศดังกล่าว
- **เมษายน 2024:** เว็บไซต์บันเทิงของจีนถูกโจมตีด้วย 4.2 ล้าน RPS จาก 2,600 IP ในประเทศจีนและสหรัฐอเมริกา เป็นระยะเวลานานเกือบห้าชั่วโมง

อุตสาหกรรมที่ตกเป็นเป้าหมายมากที่สุด

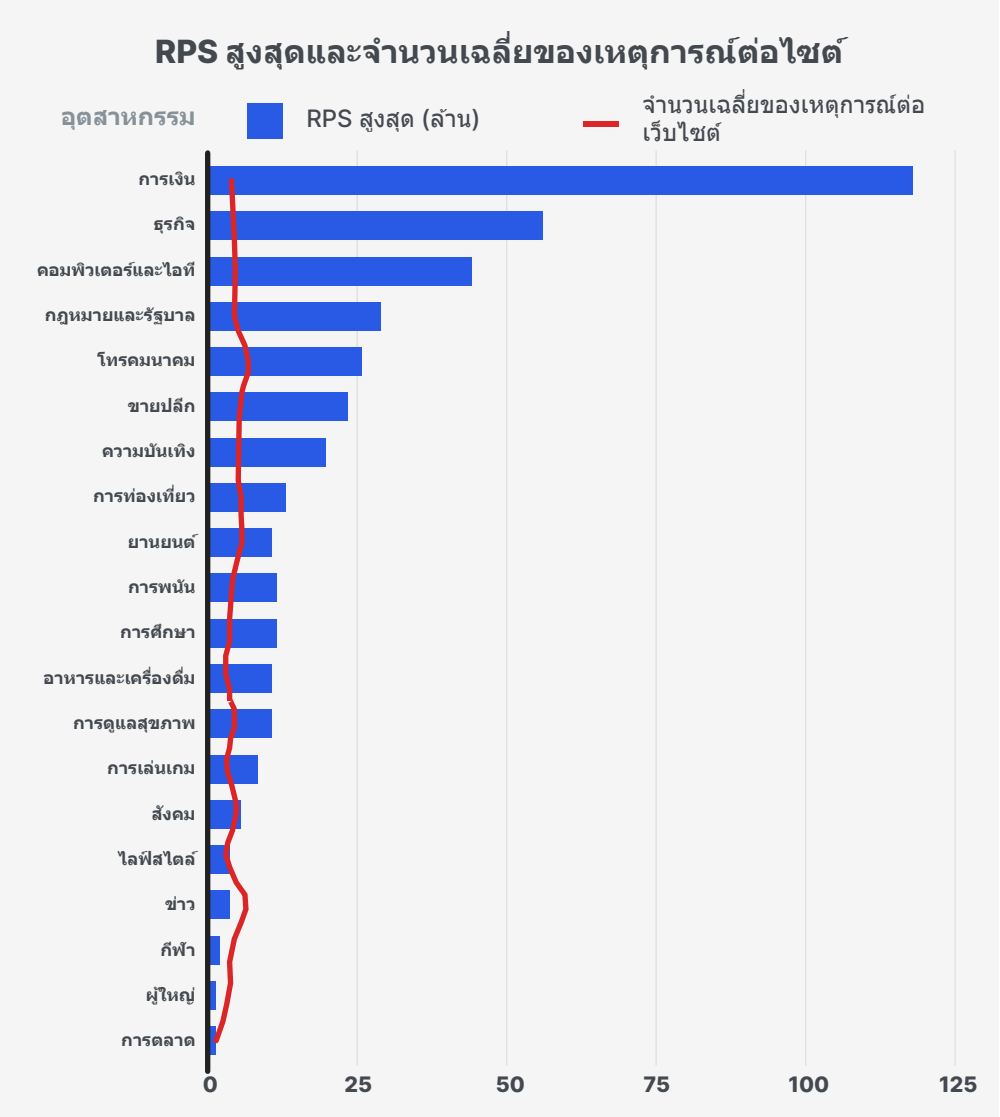
ในช่วงครึ่งแรกของปี 2024 บริการทางการเงิน (23.8%), ธุรกิจ (20.1%) และระบบโทรคมนาคมและ ISP (12.3%) เป็นอุตสาหกรรมที่ตกเป็นเป้าหมายมากที่สุด ซึ่งคิดเป็นเกือบ 60% ของการโจมตี DDoS แบบเลเยอร์ 7 ทั้งหมด



อุตสาหกรรมที่ตกเป็นเป้าหมายของการโจมตีแบบ DDoS ที่ทรงพลังที่สุด

ภาคธุรกิจการเงินไม่เพียงเป็นเป้าหมายอันดับหนึ่งสำหรับผู้โจมตี DDoS เท่านั้น แต่ยังเป็นเป้าหมายของการโจมตี DDoS ที่ทรงพลังที่สุดในแง่ของคำขอต่อวินาที (Requests per Second หรือ RPS) เมื่อเป็นเรื่องของการโจมตี DDoS อาชญากรไซเบอร์จะใช้วิธีการที่ทรงพลังมากขึ้นเพื่อให้ประสบความสำเร็จในการโจมตีที่มีโอกาสทำกำไรได้มากที่สุด

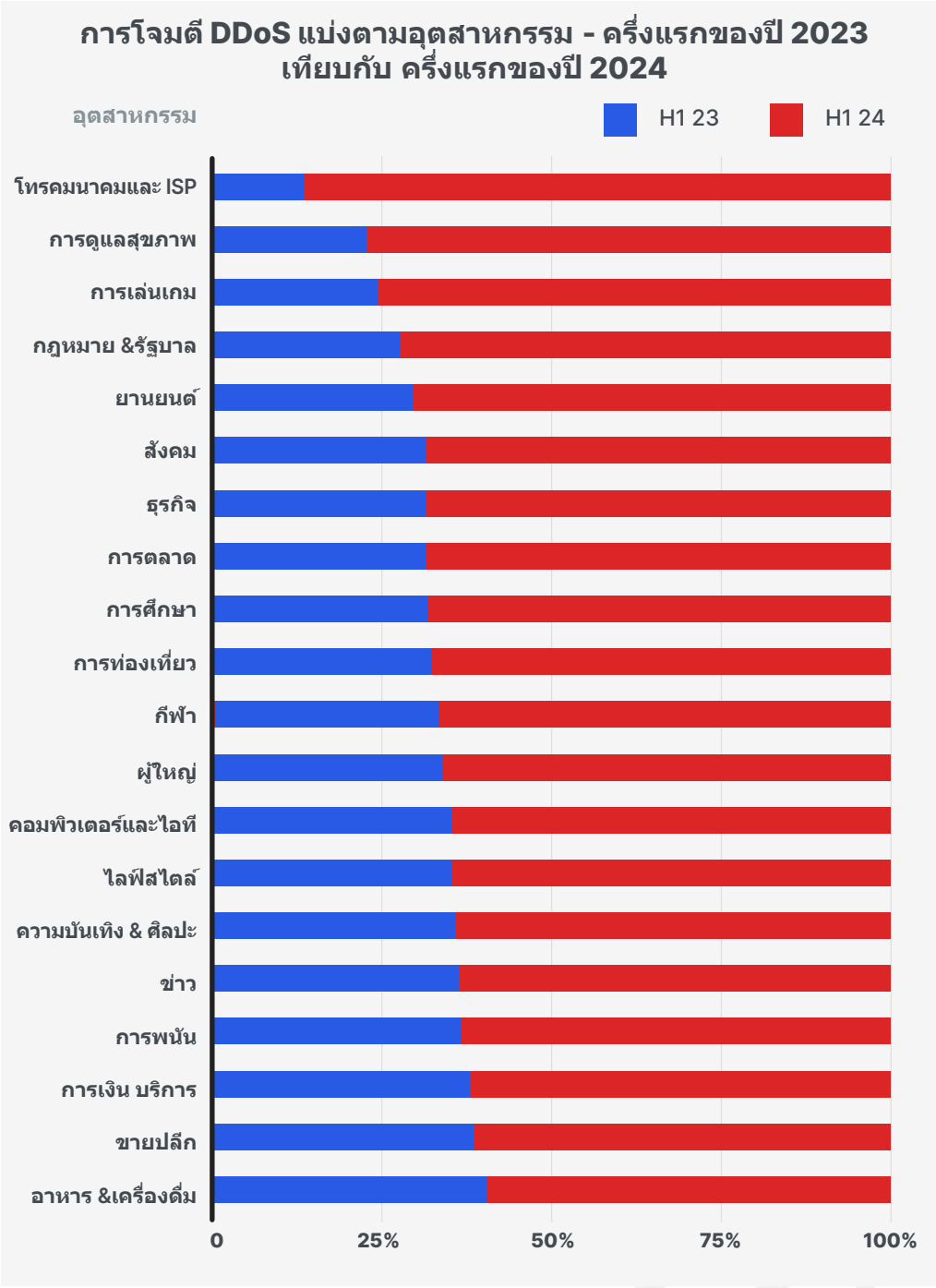
ไม่น่าแปลกใจที่การโจมตีภาคบริการทางการเงินมีปริมาณสูงถึง 118 ล้าน RPS รวมกันใน H1 24 โดยมีภาคธุรกิจและไอทีเข้ามาอยู่ในอันดับที่สองและสามตามลำดับ



อุตสาหกรรมที่ประสบกับการโจมตี DDoS เพิ่มขึ้นสูงสุด

เมื่อเปรียบเทียบครึ่งแรกของปี 2024 กับช่วงเดียวกันของปีที่แล้ว มีการโจมตี DDoS เพิ่มขึ้นอย่างมีนัยสำคัญในหลายอุตสาหกรรม อุตสาหกรรมโทรคมนาคมและ ISP มีอัตราการเติบโตของการโจมตีสูงสุดต่อปี โดยเพิ่มขึ้น 548% ในการโจมตี DDoS แบบแอปพลิเคชันเลเยอร์ อุตสาหกรรมการดูแลสุขภาพพบการโจมตีมากขึ้น 236% และตัวเลขการโจมตีของอุตสาหกรรมเกมเพิ่มขึ้น 208%

การโจมตีทางไซเบอร์ต่อผู้ให้บริการอินเทอร์เน็ต (ISP) เป็นภัยคุกคามที่ร้ายแรงและต่อเนื่องขององค์กรและหน่วยงานสาธารณะ ISP ถือเป็นโครงสร้างพื้นฐานที่สำคัญระดับประเทศ โดยทำหน้าที่ให้บริการอินเทอร์เน็ตแก่ธุรกิจและบุคคลธรรมดา เพื่อให้ทุกฝ่ายสามารถให้บริการออนไลน์และดำเนินงานทางเศรษฐกิจได้อย่างต่อเนื่อง ด้วยเหตุผลเหล่านี้ ISP จึงเป็นเป้าหมายสูงสุดสำหรับอาชญากรไซเบอร์ที่มีเจตนาทำการหยุดชะงักประสบปัญหาสูงสุด



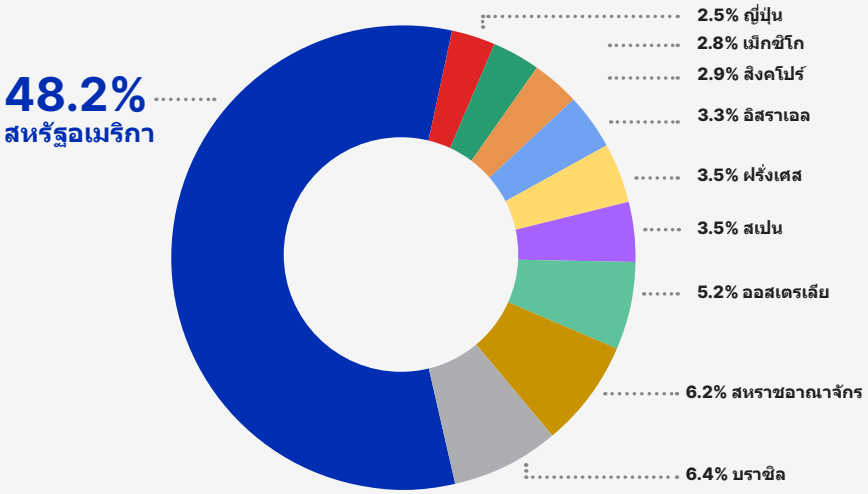
การโจมตี DDoS ต่อธุรกิจค้าปลีกเพิ่มขึ้น 61%

แม้ว่าจะไม่ได้อยู่ใน 10 อันดับแรก แต่การโจมตี DDoS ต่อภาคธุรกิจค้าปลีกได้เพิ่มขึ้นเกือบ 61% นับตั้งแต่ปีที่แล้ว ซึ่งสะท้อนให้เห็นถึงการเพิ่มขึ้นของอาชญากรรมไซเบอร์ที่มุ่งเป้าไปที่แพลตฟอร์มอีคอมเมิร์ซและการทำธุรกิจค้าปลีกออนไลน์ แนวโน้มนี้ยิ่งทำให้เห็นความเปราะบางที่เพิ่มขึ้นของภาคอุตสาหกรรม เนื่องจากอาชญากรไซเบอร์มุ่งที่จะขัดขวางการขายและทำลายข้อมูลลูกค้า

ประเทศที่ตกเป็นเป้าหมายมากที่สุด

สหรัฐอเมริกายังคงตกเป็นเป้าหมายหลักของการโจมตี DDoS โดยเกือบครึ่งหนึ่งของการโจมตีแอปพลิเคชันเลเยอร์ทั้งหมดในครึ่งแรกของปี 2024 มีเป้าเป็นสหรัฐอเมริกา นอกจากนี้ บราซิล สหราชอาณาจักร และออสเตรเลียก็ประสบกับการโจมตีที่สำคัญเช่นกัน แต่ในระดับที่น้อยกว่า

การโจมตี DDoS เลเยอร์ 7 - 20 ประเทศที่ถูกโจมตีมากที่สุดในครึ่งแรกของปี 2024



ประเทศและเขตแดนที่ตกเป็นเป้าหมายน้อยที่สุดในช่วงเวลานี้ ได้แก่ สโลวาเกีย เซเนกัล และมัลดีฟส์

เวกเตอร์การโจมตีใหม่ที่บรรเทาลงได้

เวกเตอร์การโจมตีใหม่มีความสำคัญสำหรับอาชญากรไซเบอร์เสมอ เนื่องจากเวกเตอร์เหล่านี้ช่วยให้พวกเขามีคลังอาวุธในการโจมตีเพิ่มเติม และช่วยให้สามารถสร้างการโจมตีที่ซับซ้อนและละเอียดอ่อนได้มากขึ้นได้

ในปีนี้เราได้สังเกตเห็นเวกเตอร์การโจมตี DDoS แบบแอปพลิเคชันเลเยอร์ใหม่ที่สำคัญสองเวกเตอร์:

การโจมตีแบบ HTTP/2 Rapid Reset

HTTP/2 Rapid Reset เป็นประเภทของการโจมตีที่ค่อนข้างใหม่ ซึ่งเห็นครั้งแรกในปี 2023 วิธีนี้จะเป็นการปฏิเสธความเปราะบางของบริการที่ถูกจัดหมวดหมู่เป็น CVE-2024-44487 ที่ส่งผลกระทบต่อโปรโตคอล HTTP2 ทำให้ไคลเอ็นต์ http สามารถเปิดสตรีมและยกเลิกได้ทันทีหลังจากนั้น กิจกรรมที่เป็นการเปิด/ยกเลิกซ้ำไปซ้ำมานี้ เมื่อดำเนินการในปริมาณมาก จะทำให้เซิร์ฟเวอร์ทำงานหนักเกินไป

การโจมตีแบบ HTTP/2 Continuation Frame

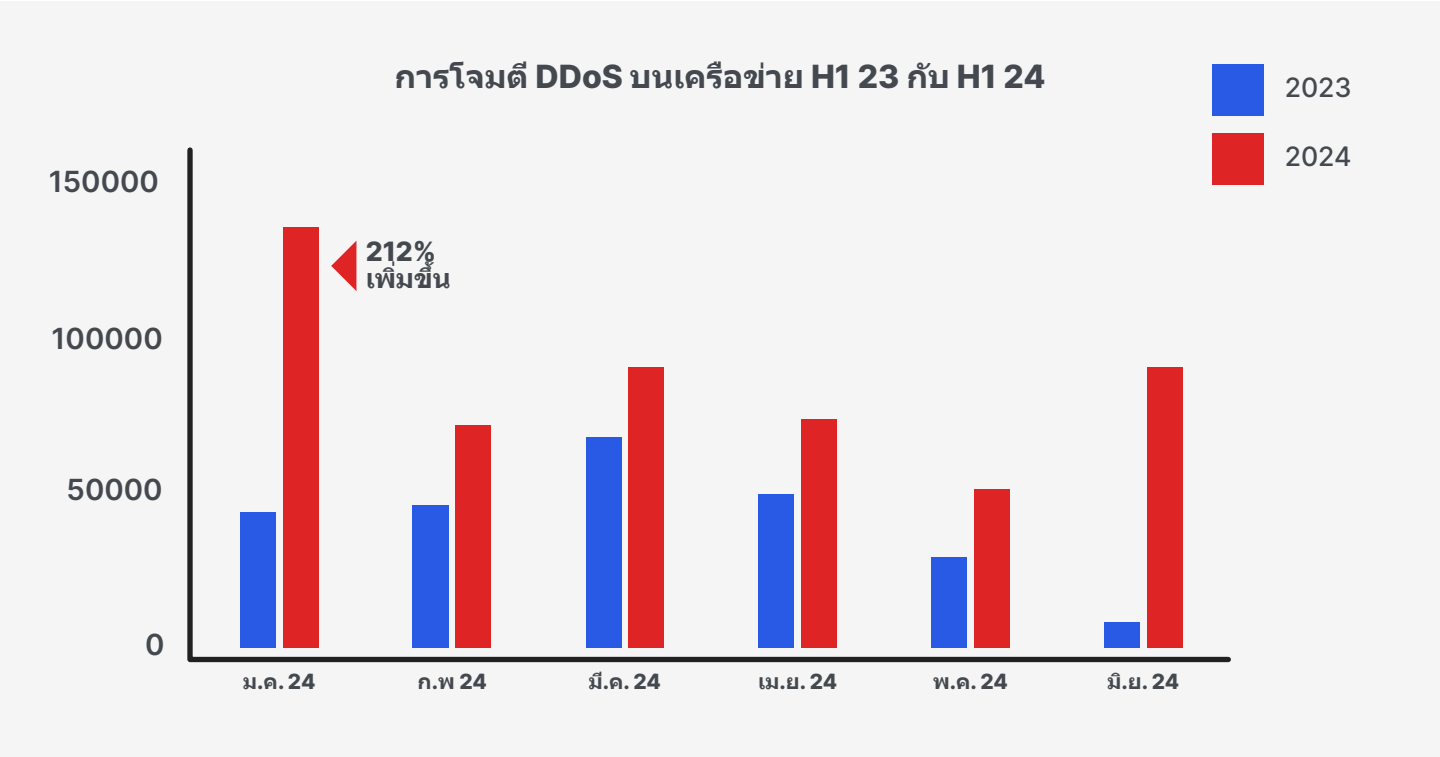
เมื่อเร็วๆ นี้ มีการโจมตีแบบ **HTTP/2 Continuation Frame เพิ่มมากขึ้น** ซึ่งเป็นการโจมตี DDoS เลเยอร์ 7 ในรูปแบบใหม่ การโจมตีเหล่านี้ใช้ประโยชน์จากช่องโหว่ในโปรโตคอล HTTP/2 โดยการส่งสตรีมอย่างต่อเนื่องของคำขอขนาดเล็กที่แยกส่วนไปยังเซิร์ฟเวอร์ที่มีปริมาณงานท่วมท้น วิธีนี้ช่วยให้ผู้โจมตีสามารถเลี่ยงการป้องกันแบบเดิมและทำให้เกิดการหยุดชะงักอย่างมีนัยสำคัญด้วยปริมาณการจราจรที่ค่อนข้างต่ำ การเพิ่มจำนวนมากขึ้นของการโจมตีที่ซับซ้อนเหล่านี้ ยิ่งทำให้เราเห็นถึงภูมิทัศน์ที่เปลี่ยนไปของภัยคุกคาม และความจำเป็นที่จะต้องมีมาตรการรักษาความปลอดภัยที่มีประสิทธิภาพมากขึ้น เพื่อปกป้องโครงสร้างพื้นฐานที่สำคัญ

การโจมตี DDoS แบบเลเยอร์เครือข่าย (เลเยอร์ 3 และ 4)

การโจมตี DDoS แบบเลเยอร์เครือข่ายมีจำนวนเพิ่มมากขึ้นเมื่อเทียบปีต่อปี

การโจมตี DDoS แบบเลเยอร์ 3 และ 4 เพิ่มขึ้น 111% ใน H1 2024 เมื่อเทียบกับปีที่แล้ว โดยการโจมตีที่โดดเด่นที่สุดจะอยู่ได้นานกว่าสี่ชั่วโมงและมีตัวเลขสูงถึง 731 Gbps ในเดือนมีนาคม 2024

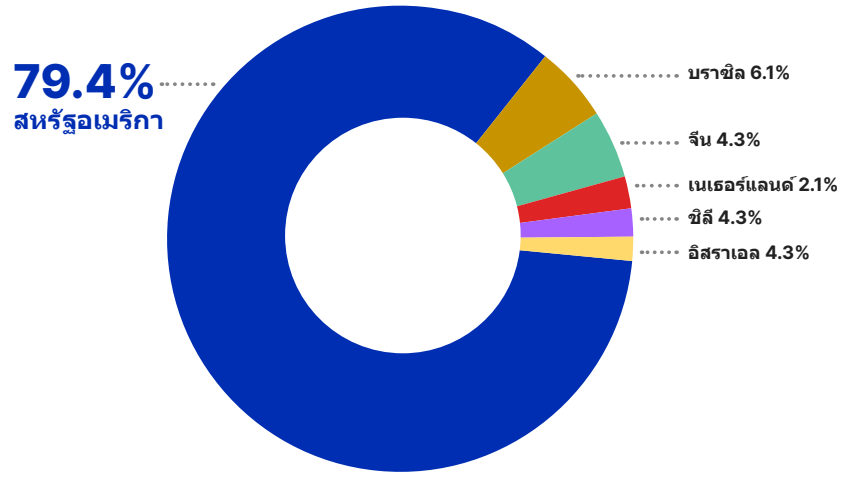
การเพิ่มขึ้นที่สำคัญที่สุดของจำนวนการโจมตี DDoS แบบเลเยอร์ 3 และ 4 เกิดขึ้นในเดือนมกราคม 2024 เมื่อการโจมตีเพิ่มขึ้น 212% เทียบกับเดือนเดียวกันของปีที่แล้ว



ประเทศที่ตกเป็นเป้าหมายมากที่สุดสำหรับการโจมตี DDoS แบบเลเยอร์เครือข่าย

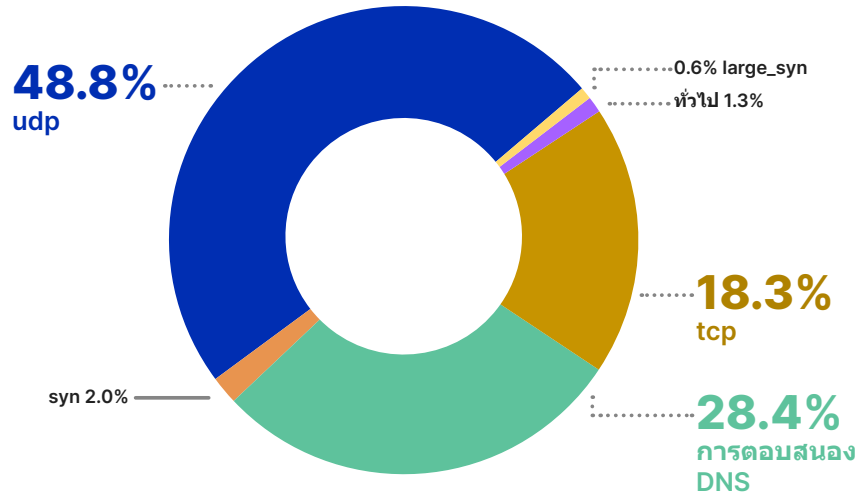
ใน H1 2024 เกือบ 80% ของการโจมตีทั้งหมดมีเป้าหมายเป็นเครือข่ายในสหรัฐอเมริกา โดยมีบราซิล จีน และเนเธอร์แลนด์เป็นประเทศเป้าหมายอันดับรองลงมา

การโจมตี DDoS เลเยอร์ 3 และ 4 - ประเทศที่ถูกโจมตีมากที่สุด



ประเทศที่ตกเป็นเป้าหมายน้อยที่สุด ได้แก่ แอฟริกาใต้ เวเนซุเอลา และบาห์เรน

ปริมาณการโจมตีแบบเลเยอร์เครือข่าย (Gbps) โดยเวกเตอร์

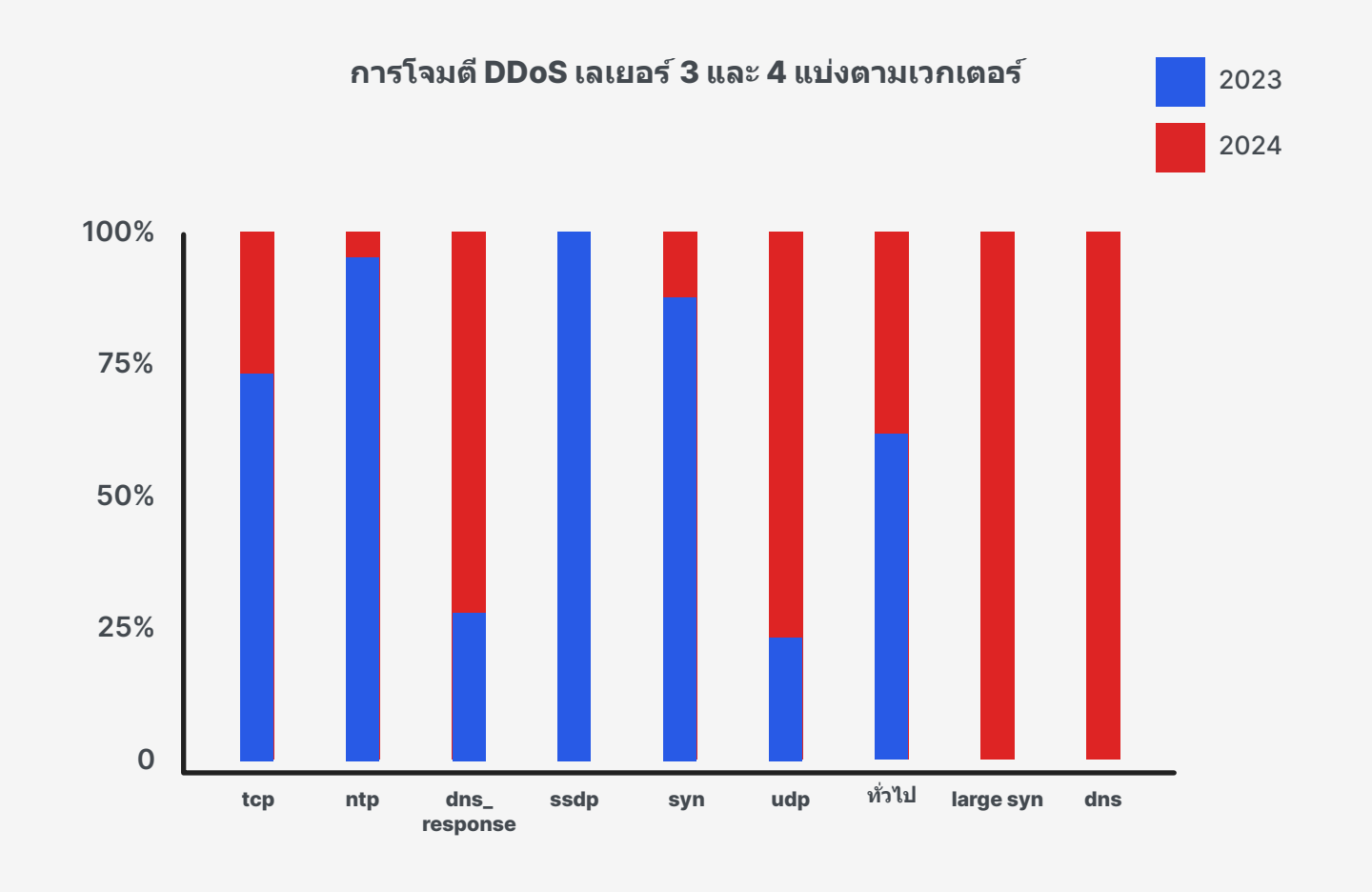


แผนภูมิข้างต้นตั้งแต่เดือนพฤษภาคม 2024 แสดงให้เห็นว่าการโจมตีด้วยการตอบสนองแบบ DNS และการโจมตีแบบ UDP มีส่วนสำคัญต่อการโจมตีส่วนใหญ่แบบเลเยอร์เครือข่ายเวกเตอร์ทั้งสองกลุ่มมีการเติบโตอย่างมีนัยสำคัญตลอดทั้งปี[3]

เวกเตอร์การโจมตีแบบเลเยอร์ 3 และ 4 ใหม่

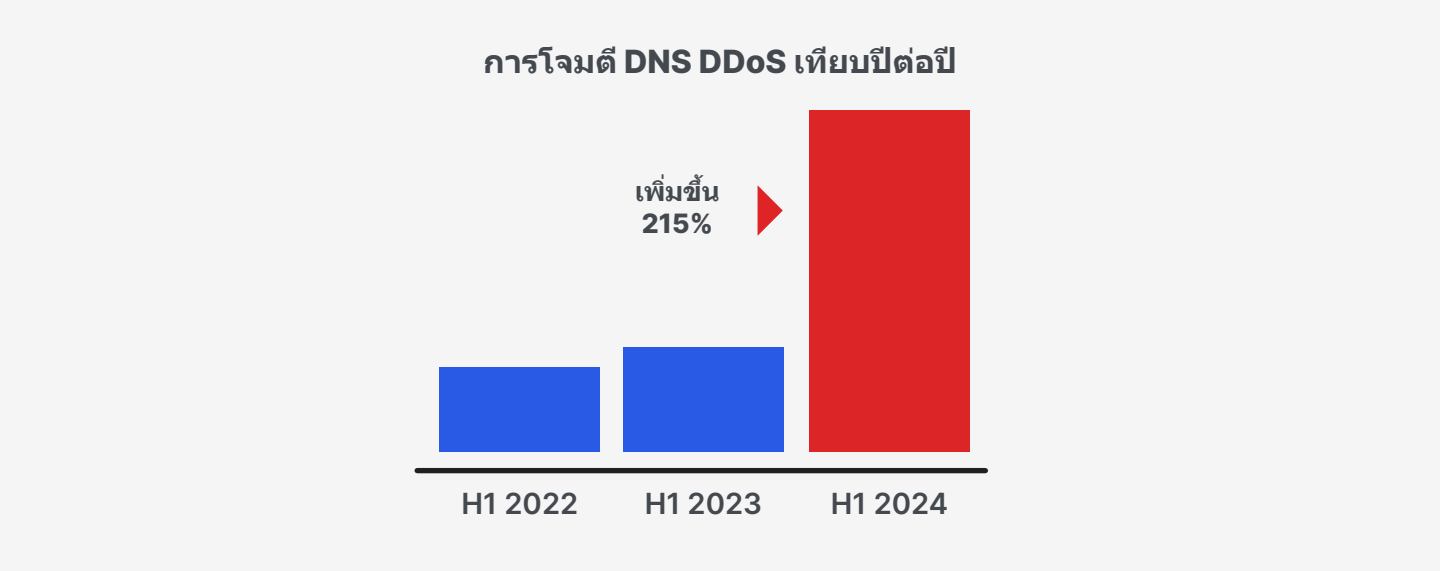
การโจมตี DoS แบบลูปแอปพลิเคชันเลเยอร์

ตามรายงานของ **The Hacker News** เวกเตอร์การโจมตีที่เพิ่งระบุพบใหม่นี้มุ่งเป้าไปที่โปรโตคอลที่ใช้ UDP ทั้งรุ่นเก่า (เช่น QOTD, Chargen, Echo) และรุ่นร่วมสมัย (เช่น DNS, NTP, TFTP) ที่ทำให้เซิร์ฟเวอร์สื่อสารได้อย่างไม่มีกำหนด เวกเตอร์นี้ค้นพบโดยนักวิจัยของ CISPA Helmholtz-Center ซึ่งอาจส่งผลต่อโฮสต์อินเทอร์เน็ตประมาณ 300,000 ราย แม้ว่า DDoS เวกเตอร์ใหม่จะถูกระบุพบในปีนี้ แต่ Imperva สังเกตว่ายังไม่มีการโจมตีแบบ DDoS loop ชั้นที่ 3/4 ในครึ่งแรกของปี 2024



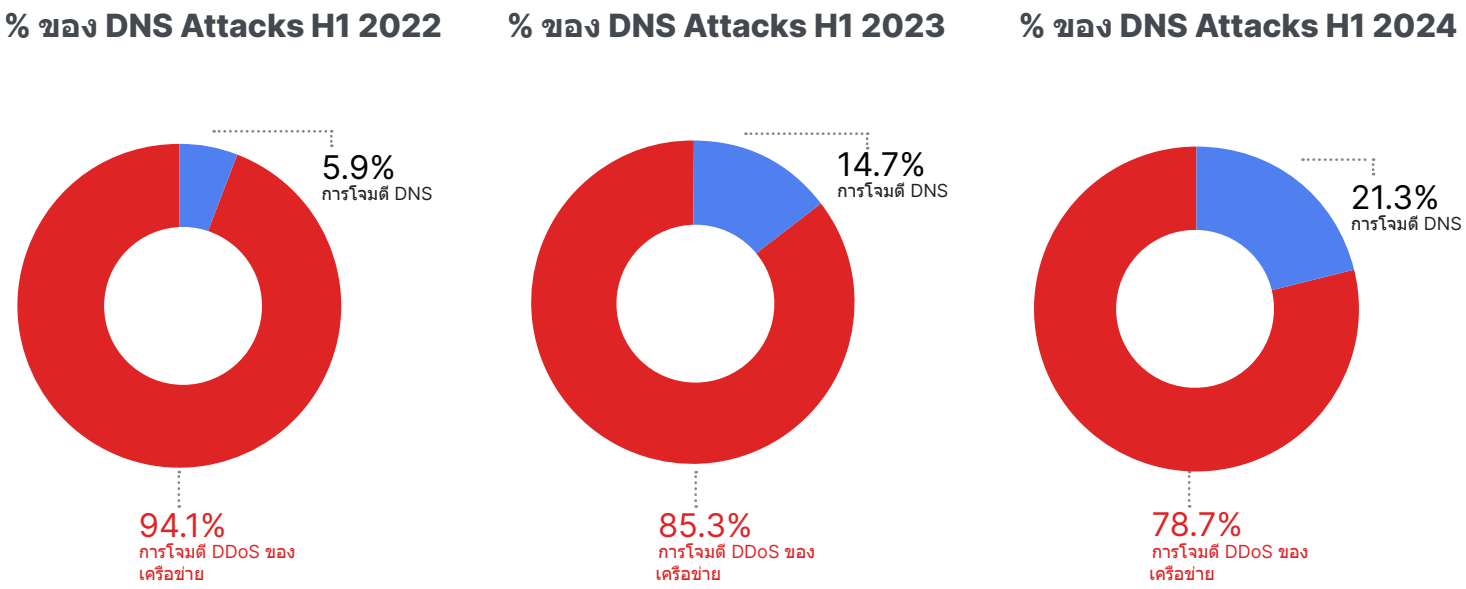
การโจมตี DNS เพิ่มขึ้น 215%

การโจมตี DNS DDoS กำลังเติบโตอย่างมีนัยสำคัญ เมื่อเปรียบเทียบ H1 2024 กับช่วงเดียวกันของปีที่แล้ว การโจมตี DNS DDoS เพิ่มขึ้น 215%

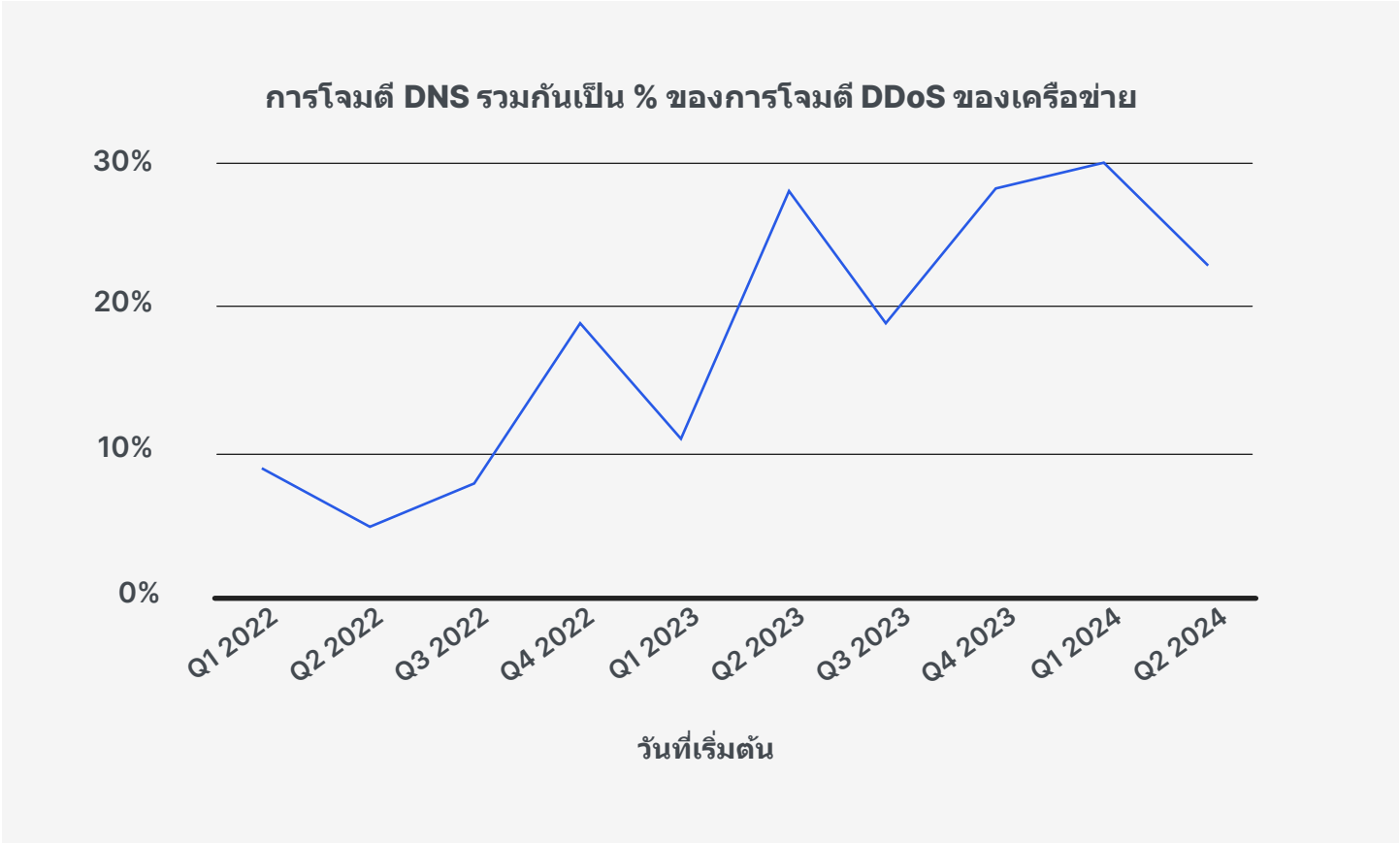


DNS กำลังเข้าไปแทรกซึมเป็นส่วนหนึ่งของภูมิทัศน์การโจมตี DDoS บนเครือข่าย

การโจมตี DNS เป็นเวกเตอร์ที่มีเปอร์เซ็นต์ของการโจมตี DDoS ต่อเครือข่ายโดยรวมต่อปีที่เพิ่มมากขึ้น หลังจากที่มีตัวเลขคิดเป็นเพียง 6% ของการโจมตี DDoS ต่อเครือข่ายทั้งหมดในปี H1 2022 แต่ในปี H1 2024 การโจมตี DNS DDoS คิดเป็นมากกว่า 21% ของการโจมตี DDoS ต่อเครือข่าย



ทั้งเวกเตอร์ DNS Request และเวกเตอร์ DNS Response มีอัตราการเติบโตตามเปอร์เซ็นต์ของจำนวนรวมของการโจมตี DDoS ต่อเครือข่ายรวมกัน ตามแผนภูมิด้านล่าง

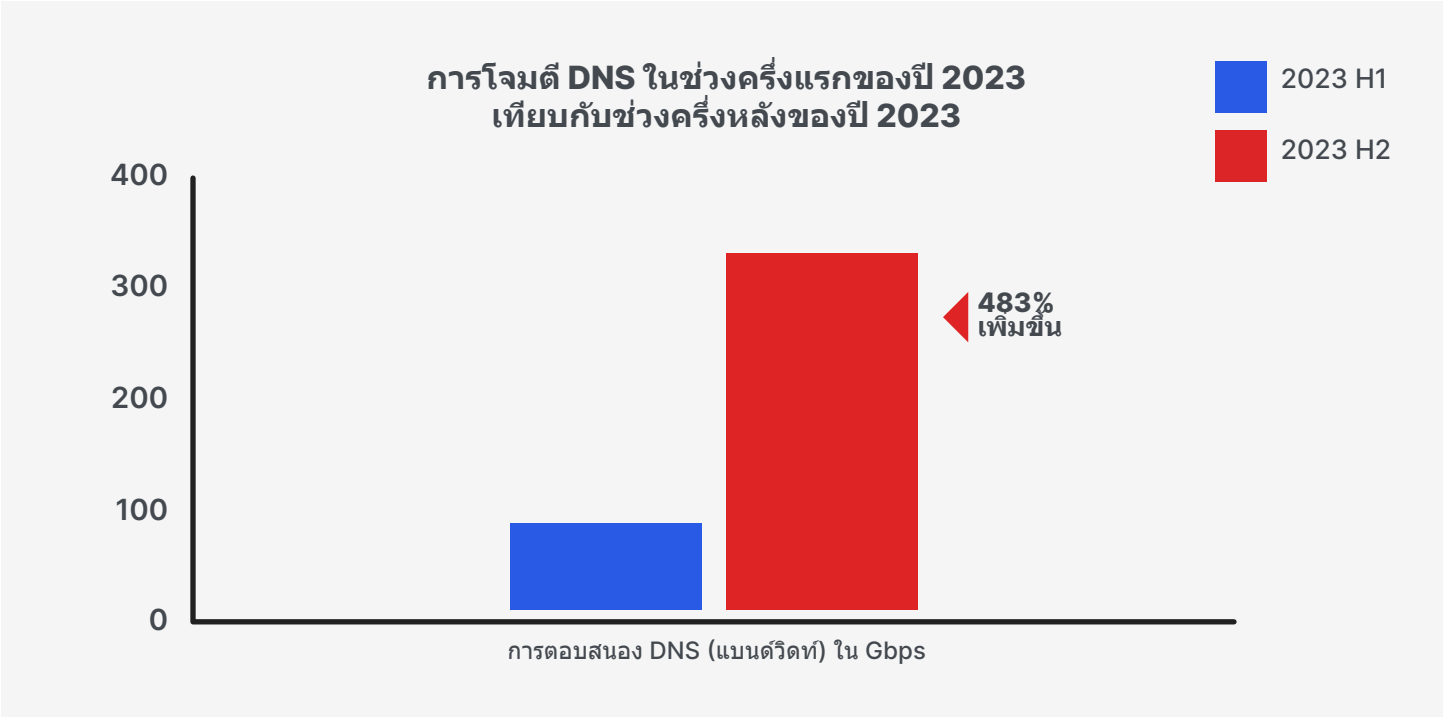


ทั้งเวกเตอร์ DNS Request และเวกเตอร์ DNS Response มีอัตราการเติบโตตามเปอร์เซ็นต์ของจำนวนรวมของการโจมตี DDoS ต่อเครือข่ายรวมกัน

การโจมตี DNS DDoS ที่เพิ่มขึ้นในแง่ของขนาด

การโจมตีแบบขยาย DNS สามารถทำให้เซิร์ฟเวอร์ถูกถล่มด้วยควิรีจำนวนมหาศาล ซึ่งมักจะเกิดจากบอทเน็ต ทำให้เกิดการปฏิเสธการให้บริการที่นำไปสู่การถดถอยของคุณภาพการให้บริการ หรือการหยุดทำงานของเซิร์ฟเวอร์หรือเครือข่ายที่ถูกโจมตี

ในปี 2023 การโจมตี DNS Amplification เพิ่มขึ้นในแง่ของแบนด์วิดท์สูงสุดลดลงเริ่มต้นที่ 59 Gbps ใน H1 2023 เมื่อเทียบกับการตัวเลขที่แตะถึง 344 Gbps ใน H2 2023



แบนด์วิดท์สูงถึง 59 Gbps ในครึ่งแรกของปี 2023 เทียบกับ 344 Gbps ในครึ่งหลังของปี 2023

การเพิ่มขึ้นของจำนวนและความรุนแรงของการโจมตีบนเซิร์ฟเวอร์ DNS นั้นมีสาเหตุมาจากหลายปัจจัย รวมถึงบทบาทที่สำคัญในการใช้งานอินเทอร์เน็ต การแพร่ขยายของบอตเน็ต เทคนิคการโจมตีที่พัฒนายิ่งขึ้น และหลักปฏิบัติด้านความปลอดภัยที่อ่อนแอ แรงจูงใจทางการเงิน การเมือง และการเพิ่มขึ้นของอุปกรณ์ IoT ที่ไม่ปลอดภัยยังผลักดันให้เกิดการโจมตีเหล่านี้ ซึ่งทำให้การรักษาความปลอดภัยของ DNS กลายเป็นข้อกังวลอย่างมาก

แบนด์วิดท์การโจมตี DNS Amplification โดยเฉลี่ยในช่วงครึ่งหลังของปี 2023 อยู่ที่ 59 กิกะบิตต่อวินาที เทียบกับ **344 กิกะบิตต่อวินาที**ในช่วงครึ่งหลังของปี 2023 เพิ่มขึ้น**483%**

กลุ่มแฮ็กทิวิสต์มักใช้การโจมตี DDoS

เพื่อทำให้โครงสร้างพื้นฐานที่สำคัญหยุดชะงัก เมื่อเร็วๆ นี้ NoName57(16) ซึ่งเป็นกลุ่มแฮ็กทิวิสต์ของรัสเซียที่เกี่ยวพันกับความตึงเครียดทางภูมิศาสตร์การเมือง ได้ขู่จะสร้างปัญหาต่อโครงสร้างพื้นฐานอินเทอร์เน็ตของยุโรปในระหว่างการเลือกตั้งของสหภาพยุโรป ตามที่รายงานโดย **The Register** กลุ่มนี้ถือกำเนิดขึ้นหลังเหตุการณ์การรุกรานยูเครน และยุทธวิธีที่พวกเขานิยมใช้อย่าง DDoS ก็ยังคงเป็นเครื่องมือที่มีศักยภาพในการสร้างความปั่นป่วน

กลุ่มเหล่านี้ เช่น Anonymous Sudan และ NoName57(16) ยังเป็นตัวการสำคัญของภัยคุกคามที่เกิดขึ้นอย่างต่อเนื่องและมีการพัฒนาเพิ่มมากขึ้นในโลกไซเบอร์ ในช่วงต้นปี 2024 Imperva ตอบสนองต่อการโจมตี DDoS จำนวนมากบนโครงสร้างพื้นฐานที่สำคัญระดับชาติ เห็นได้ชัดว่าในเดือนมีนาคม 2024 Imperva ได้ขัดขวางการโจมตีสนามบินยุโรปที่สำคัญแห่งหนึ่ง ซึ่งตัวเลขคำขอต่อวินาทีเกือบจะแตะ 1 ล้าน RPS สนามบินเป็นเป้าหมายหลักเนื่องจากบทบาทของพวกเขาในฐานะศูนย์กลางแห่งชาติที่สำคัญ ซึ่งการหยุดชะงักสามารถสร้างความวุ่นวายด้านโลจิสติกส์ได้

นอกจากนี้ Imperva ยังลดการโจมตี DDoS ที่เกิดขึ้นซ้ำ ๆ กับหน่วยงานการสื่อสารในเอเชีย การโจมตีหนึ่งครั้งมียอดสูงสุดอยู่ที่ 2.5 ล้าน RPS ในขณะที่หน่วยงานเป้าหมายอีกหน่วยงานหนึ่งต้องเผชิญกับการโจมตี 1.5 ล้าน RPS นอกจากนี้ สำนักงานรัฐบาลในญี่ปุ่นยังสามารถป้องกันจากการโจมตีได้เป็นจำนวนมากถึง 780,000 RPS ในเดือนกุมภาพันธ์

โครงสร้างพื้นฐานที่สำคัญของประเทศได้ตกเป็นเป้าหมายการโจมตี DDoS บ่อยครั้ง

- หน่วยงานด้านการสื่อสารแห่งชาติ
- ออกอากาศ
- สนามบินสื่อ
- โรงพยาบาล
- ผู้ให้บริการอินเทอร์เน็ต
- เจ้าหน้าที่ของรัฐ

การโจมตี DDoS ในการแข่งขันกีฬารายการสำคัญ

ในเดือนกุมภาพันธ์ 2024 Imperva ได้สกัดกั้นการโจมตี DDoS ครั้งใหญ่ที่สุดของปี ซึ่งมีตัวเลขสูงถึง 4.7 ล้าน RPS หนึ่งแรงจูงใจที่เป็นไปได้สำหรับการโจมตีที่มีเป้าหมายเป็นเว็บไซต์เกมของอินโดนีเซีย อาจเป็นการแข่งขันฟุตบอล AFC Cup ซึ่งกำลังเกิดขึ้นในเวลานั้น แฮ็กทิวิสต์มักจะใช้ประโยชน์จากเหตุการณ์สำคัญเพื่อเพิ่มผลกระทบจากการโจมตีของตนให้รุนแรงที่สุด และเมื่อฝรั่งเศสและเยอรมนีเป็นเจ้าภาพจัดการแข่งขันกีฬาโอลิมปิกและ UEFA Europe 2024 ตามลำดับ อุตสาหกรรมที่เกี่ยวข้องจึงมีความเสี่ยงเพิ่มขึ้น ตัวอย่างหนึ่งก็คือ**ช่องกีฬาของโปแลนด์ได้ถูกโจมตีโดยวิธี DDoS** ในระหว่างการแข่งขัน Euro 2024 ของทีมชาติกับเนเธอร์แลนด์

การศึกษาวิจัยภัยคุกคามของเราบ่งชี้ว่าการโจมตีแบบ DDoS เลเยอร์ 7 ต่อเว็บไซต์การท่องเที่ยว กีฬา ความบันเทิง และการพนันในยุโรปเพิ่มขึ้น 89% เมื่อเทียบกับปีที่แล้ว โดยมีการโจมตีสูงสุดถึง 1.5 ล้าน RPS

สำหรับข้อมูลเชิงลึกเพิ่มเติมเกี่ยวกับผลกระทบของการโจมตี DDoS ต่อโครงสร้างพื้นฐานที่สำคัญในระหว่างการแข่งขันกีฬาครั้งสำคัญ โปรดอ่านบล็อกของเรา: **เราคือผู้ปกป้องมหกรรมกีฬาประจำฤดูร้อนในยุโรป - การรักษาความปลอดภัยมีความหมายอย่างไร**

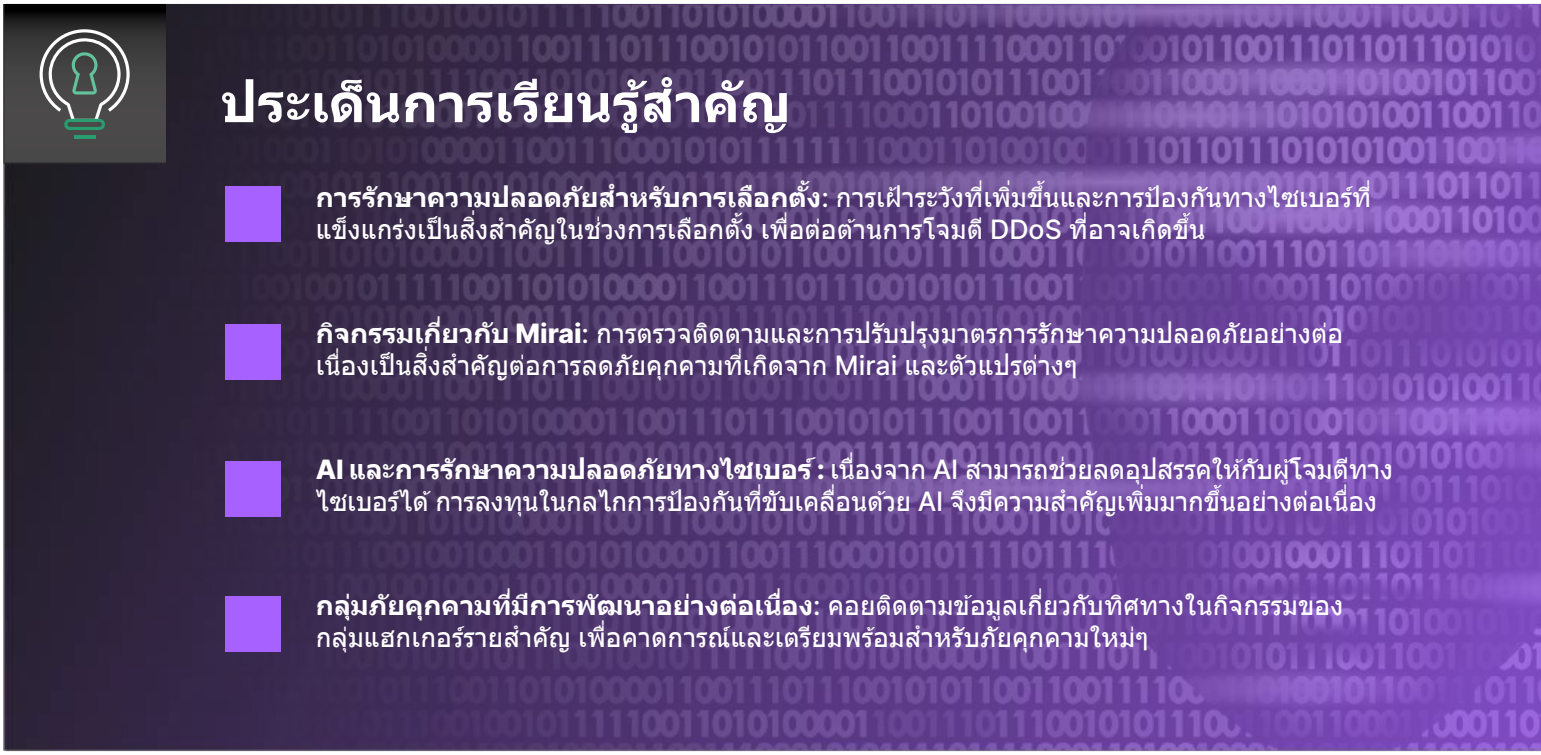
แนวโน้ม DDoS ที่คาดการณ์ไว้และอนาคตที่คาดหมายสำหรับปี 2024

การโจมตี DDoS ที่เกี่ยวข้องกับการเลือกตั้ง: ปี 2024 เป็นปีแห่งการเลือกตั้งครั้งสำคัญทั่วโลก เกือบครึ่งหนึ่งของประชากรโลกจะต้องเข้าคูหาเพื่อแสดงสิทธิ์ออกเสียงของตนเอง การเลือกตั้งมักเกิดขึ้นพร้อมกับการโจมตีแบบ DDoS ที่มีแรงขับเคลื่อนจากกิจกรรมของแฮ็กทิวิสต์และความไม่สงบทางการเมือง ตัวอย่างเช่น กลุ่มแฮ็กทิวิสต์ที่สนับสนุนรัสเซีย NoName57(16) ก่อตั้งขึ้นหลังการรุกรานของยูเครนและมีเป้าหมายการโจมตีเป็นโครงสร้างพื้นฐานอินเทอร์เน็ตของยุโรปในระหว่างการเลือกตั้งของ EU เหตุการณ์ดังกล่าวเป็นตัวอย่างให้เราเห็นว่าความตึงเครียดของการเมืองในทางภูมิศาสตร์สามารถผลักดันให้การโจมตี DDoS เพิ่มจำนวนมากขึ้นได้อย่างไร

บอทเน็ต Mirai ต่างๆ: ในช่วงต้นปี 2024 งานวิจัยของเราสังเกตพบการส่งมัลแวร์บอทเน็ต Mirai ไปยังเว็บไซต์มากกว่า 1,200 แห่งผ่านช่องโหว่ของเว็บ แม้ว่าเป้าหมายหลักยังคงไม่ชัดเจน แต่ประวัติของ Mirai ในการดำเนินการโจมตี DDoS ขนาดใหญ่นั้นมีหลักฐานที่ชัดเจน ซึ่งเป็นการส่งสัญญาณเตือนถึงภัยคุกคามที่อาจเกิดขึ้นในอนาคต อ่านบล็อกฉบับเต็มได้ที่นี่

AI ลดอุปสรรคในการโจมตี: AI ทำให้ผู้โจมตีที่มีทักษะไม่สูงสามารถใช้ประโยชน์จากช่องโหว่ใหม่ได้อย่างรวดเร็วและง่ายขึ้น ตัวอย่างเช่น เครื่องมือ AI สามารถทำให้การสร้างและการใช้งานการโจมตี DDoS ที่ซับซ้อนเป็นไปโดยอัตโนมัติ ทำให้แฮกเกอร์มือใหม่สามารถดำเนินการโจมตีที่ทรงพลังได้ แนวโน้มนี้จะเพิ่มโอกาสของการโจมตี DDoS อย่างมีนัยสำคัญโดยใช้บอทเน็ตที่มีการขยายประสิทธิภาพด้วย AI เช่น Mirai สายพันธุ์ใหม่ที่อาจเกิดขึ้น

การเปลี่ยนแปลงในกลุ่มการแฮ็ก DDoS: ภูมิทัศน์ของภัยคุกคามทางไซเบอร์มีการเปลี่ยนแปลงที่ก้าวหน้ามากขึ้น โดยเฉพาะการหายตัวไปของกลุ่มการแฮ็ก DDoS ที่มีชื่อเสียงอย่าง Anonymous Suda พวกเขาขึ้นชื่อในเรื่องการโจมตีที่รุนแรง โดยเฉพาะอย่างยิ่งกับเว็บไซต์ของอิสราเอล การเงียบหายไปอย่างฉับพลันของพวกเขาได้ทิ้งช่องว่างไว้อย่างเห็นได้ชัด ในเดือนกุมภาพันธ์ 2024 พวกเขาอ้างความรับผิดชอบสำหรับการโจมตี DDoS บน ChatGPT ของ OpenAI ซึ่งเรียกร้องให้มีการเปลี่ยนแปลงพฤติกรรมของแชทบอท ท่ามกลางความตึงเครียดทางการเมืองทางภูมิศาสตร์ นับตั้งแต่นั้นมา กิจกรรมของพวกเขาได้ยุติลง ซึ่งอาจเชื่อมโยงกับเหตุการณ์สำคัญเหล่านี้



แนวทางปฏิบัติที่ดีที่สุดสำหรับ DDoS เมื่อตกอยู่ภายใต้การโจมตี

- ดำเนินงานในเชิงรุก
- หากคุณไม่สามารถเข้าถึงระบบ DDoS Protection ที่เปิดใช้งานตลอดเวลาได้ โปรดตรวจสอบให้แน่ใจว่าคุณมีระบบ on-dem และการปกป้องไว้คอยรับมือ
- ดำเนินการตรวจสอบในตอนนี้และเลือกใช้วิธีการปกป้องด้วยโซลูชัน DDoS
- หากคุณพบว่าตัวเองถูกโจมตี ให้เลือกผู้ให้บริการที่สามารถให้ข้อมูลการเข้าร่วมเบื้องต้นที่รวดเร็วและง่ายดาย คุณสามารถทำบุ๊กมาร์กนน้านี้ไว้เพื่อไปเข้าถึงเราได้โดยตรงหากมีเหตุการณ์เกิดขึ้นกับคุณ
- อย่าปล่อยให้การสนทนาระหว่างทีมรักษาความปลอดภัยและทีมเครือข่ายขาดตอน
- เลือกผู้ให้บริการ DDoS ที่มีชื่อเสียง ซึ่งมีประวัติการดำเนินงานอยู่ทั่วโลกและมีความสามารถในการลดการโจมตีที่มีปริมาณสูงและซับซ้อน
- เลือกโซลูชันที่มีเวลาแฝงต่ำ พร้อมความสามารถในการบรรเทาปัญหาได้รวดเร็วและถูกต้อง

เกี่ยวกับ Imperva

18

Imperva เป็นผู้นำด้านการรักษาความปลอดภัยทางไซเบอร์ที่มีพันธกิจในการช่วยเหลือให้องค์กรสามารถปกป้องข้อมูลของตน และนำเสนอเส้นทางทั้งหมดในการปกป้องข้อมูล

ลูกค้าทั่วโลกไว้วางใจให้ Imperva ช่วยปกป้องแอปพลิเคชัน ข้อมูล และเว็บไซต์ของตนจากการโจมตีทางไซเบอร์ ด้วยแนวทางแบบเบ็ดเสร็จที่ผสมผสานความทันสมัย ความปลอดภัยของแอปพลิเคชัน และความปลอดภัยของข้อมูล Imperva จึงสามารถปกป้องบริษัทได้ในทุกขั้นตอนบนเส้นทางดิจิทัล ทีมวิจัยภัยคุกคามของ Imperva และชุมชนข่าวกรองทั่วโลกของเราช่วยให้ Imperva ก้าวล้ำนำหน้าภูมิทัศน์ของภัยคุกคาม และผสานรวมความเชี่ยวชาญล่าสุดด้านการรักษาความปลอดภัย ความเป็นส่วนตัว และการปฏิบัติตามกฎระเบียบเข้ากับโซลูชันของเราได้อย่างราบรื่น

หากต้องการข้อมูลเพิ่มเติมเกี่ยวกับ Imperva DDoS Protection โปรดเยี่ยมชมเว็บไซต์ของเรา