ผู้ให้บริการโฮสติ้ง “บูลเล็ตพรูฟ (Bulletproof)” รอยร้าวในเกราะป้องกันของโครงสร้างพื้นฐานต่ออาชญากรไซเบอร์

อาชญากรไซเบอร์ที่ประสบความสำเร็จต่างพึ่งพาโครงสร้างพื้นฐานที่ปลอดภัย ตรวจจับไม่ได้ และมีความยืดหยุ่นสูงเบื้องหลังทุกเหตุการณ์ของการบุกรุกเครือข่าย ข้อมูลประจำตัวที่ถูกขโมย การโจมตีด้วยแรนซัมแวร์ หรือการขโมยและขายข้อมูลในเว็บบอร์ดที่ผิดกฎหมาย ล้วนมีโครงสร้างพื้นฐานที่ปลอดภัยรองรับอยู่ ซึ่งช่วยให้อาชญากรไซเบอร์สามารถปฏิบัติการและยังคงซ่อนตัวอยู่ได้

อย่างไรก็ตาม การไม่ถูกตรวจจับและยากต่อการติดตามตัวได้นั้น กำลังกลายเป็นความท้าทายที่เพิ่มมากขึ้นสำหรับอาชญากรไซเบอร์ ความร่วมมือระดับโลกระหว่างรัฐบาล หน่วยงานบังคับใช้กฎหมาย และภาคเอกชนกำลังทำให้พวกเขายังคงซ่อนตัวในโลกออนไลน์ได้ยากขึ้น นอกจากนี้ อาชญากรไซเบอร์เพียงไม่กี่รายเท่านั้นที่มีทักษะและความเชี่ยวชาญที่จำเป็นในการจัดการและบำรุงรักษาโครงสร้างพื้นฐานที่ปลอดภัยได้ด้วยตนเอง ด้วยเหตุนี้ พวกเขาจึงมองหาผู้ให้บริการโครงสร้างพื้นฐานที่ผิดกฎหมาย ซึ่งสามารถให้บริการนี้แทนพวกเขา ทำให้อาชญากรไซเบอร์สามารถมุ่งเป้าไปที่เหยื่อและผลกำไรได้อย่างเต็มที่

‘อาชญากรรมทางไซเบอร์ในรูปแบบการให้บริการ’ (Cybercrime-as-a-service) หมายถึงตลาดใต้ดินที่พัฒนาขึ้นเพื่อรองรับผู้ไม่ประสงค์ดีในโลกไซเบอร์หลากหลายประเภท ตลาดใต้ดินนี้ประกอบไปด้วยเครื่องมือ บริการ และข้อมูลที่สามารถซื้อหาได้ ซึ่งมีจำนวนเพิ่มขึ้นเรื่อย ๆ และพัฒนาอยู่ตลอดเวลา เพื่อช่วยให้อาชญากรไซเบอร์สามารถโจมตีเป้าหมายในโลกออนไลน์ได้ ผู้ที่ต้องการก่ออาชญากรรมทางไซเบอร์สามารถซื้อสิทธิ์การเข้าถึงเครือข่าย ซื้อเครื่องมือที่ช่วยในการหลีกเลี่ยงมาตรการรักษาความปลอดภัย รวมถึงซื้อมัลแวร์เพื่อนำไปใช้โจมตีเหยื่อและขโมยข้อมูลส่วนบุคคล ผู้ให้บริการโฮสติ้งบูเล็ตพรูฟ (Bulletproof Hosting: BPH) เป็นส่วนหนึ่งของระบบนิเวศนี้และให้บริการโครงสร้างพื้นฐานที่ปลอดภัยแก่อาชญากรไซเบอร์ ที่สำคัญคือ ผู้ให้บริการ BPH เพียงรายเดียวก็สามารถสนับสนุนให้อาชญากรไซเบอร์นับร้อยรายโจมตีเหยื่อเป้าหมายทั่วโลกได้โดยตรง

ผู้ให้บริการโฮสติ้ง “บูลเล็ตพรูฟ (Bulletproof)” คืออะไร?

กล่าวโดยง่ายคือ ผู้ให้บริการ BPH ให้เช่าโครงสร้างพื้นฐานแบบเสมือนจริงและ/หรือแบบกายภาพแก่อาชญากรไซเบอร์เพื่อนำไปใช้ในการปฏิบัติการ ผู้ให้บริการ BPH เป็นประเภทเฉพาะของบริการโครงสร้างพื้นฐานอินเทอร์เน็ตที่เอื้อโอกาสให้ผู้ไม่ประสงค์ดี (รวมถึงอาชญากรไซเบอร์) สามารถโฮสต์เนื้อหาที่ผิดกฎหมายและดำเนินกิจกรรมบนโลกอินเทอร์เน็ตได้

คำว่า “บูลเล็ตพรูฟ (Bulletproof)” เป็นเพียงคำโฆษณาทางการตลาดเท่านั้น ในความเป็นจริงแล้ว บริการเหล่านี้มีความเสี่ยงต่อการถูกสกัดกั้นไม่ต่างจากผู้ให้บริการโครงสร้างพื้นฐานอื่น ๆ แทนที่จะเป็นเช่นนั้น ผู้ให้บริการ BPH ปฏิเสธที่จะปฏิบัติตามคำร้องขอจากหน่วยงานบังคับใช้กฎหมายและการขอให้ลบเนื้อหาอื่น ๆ อีกทั้งยังเพิกเฉยต่อข้อร้องเรียนการใช้งานที่ผิดจากเหยื่อและต่อการแจ้งเตือนของสมาชิก ซึ่งหมายความว่า อาชญากรไซเบอร์สามารถสื่อสาร เปิดเว็บบอร์ดและเว็บไซต์ที่ผิดกฎหมาย เผยแพร่แคมเปญมัลแวร์และฟิชชิ่ง และฟอกเงินโดยไม่ต้องกลัวว่าผู้ให้บริการจะยกเลิกสัญญาเช่าของตนหากมีคำร้องขอจากหน่วยงานบังคับใช้กฎหมายหรือคำร้องขออื่น ๆ

ผู้ให้บริการ BPH มีส่วนร่วมในระบบนิเวศของอาชญากรรมทางไซเบอร์โดยรู้เห็น และเอื้อโอกาสให้เกิดอาชญากรรมทางไซเบอร์ที่ร้ายแรงตามแรงจูงใจทางการเงิน เหตุการณ์ด้านความมั่นคงทางไซเบอร์ครั้งสำคัญ ๆ ที่ส่งผลกระทบต่อองค์กรในออสเตรเลียและลูกค้าของพวกเขาหลายครั้ง เกิดขึ้นเนื่องจากอาชญากรใช้ประโยชน์จากผู้ให้บริการ BPH ผลที่ตามมาจากเหตุการณ์เหล่านี้ รวมถึงการโจมตีด้วยแรนซัมแวร์ที่สร้างความเสียหาย การขู่กรรโชกข้อมูล และการขโมยข้อมูลที่มีความอ่อนไหว

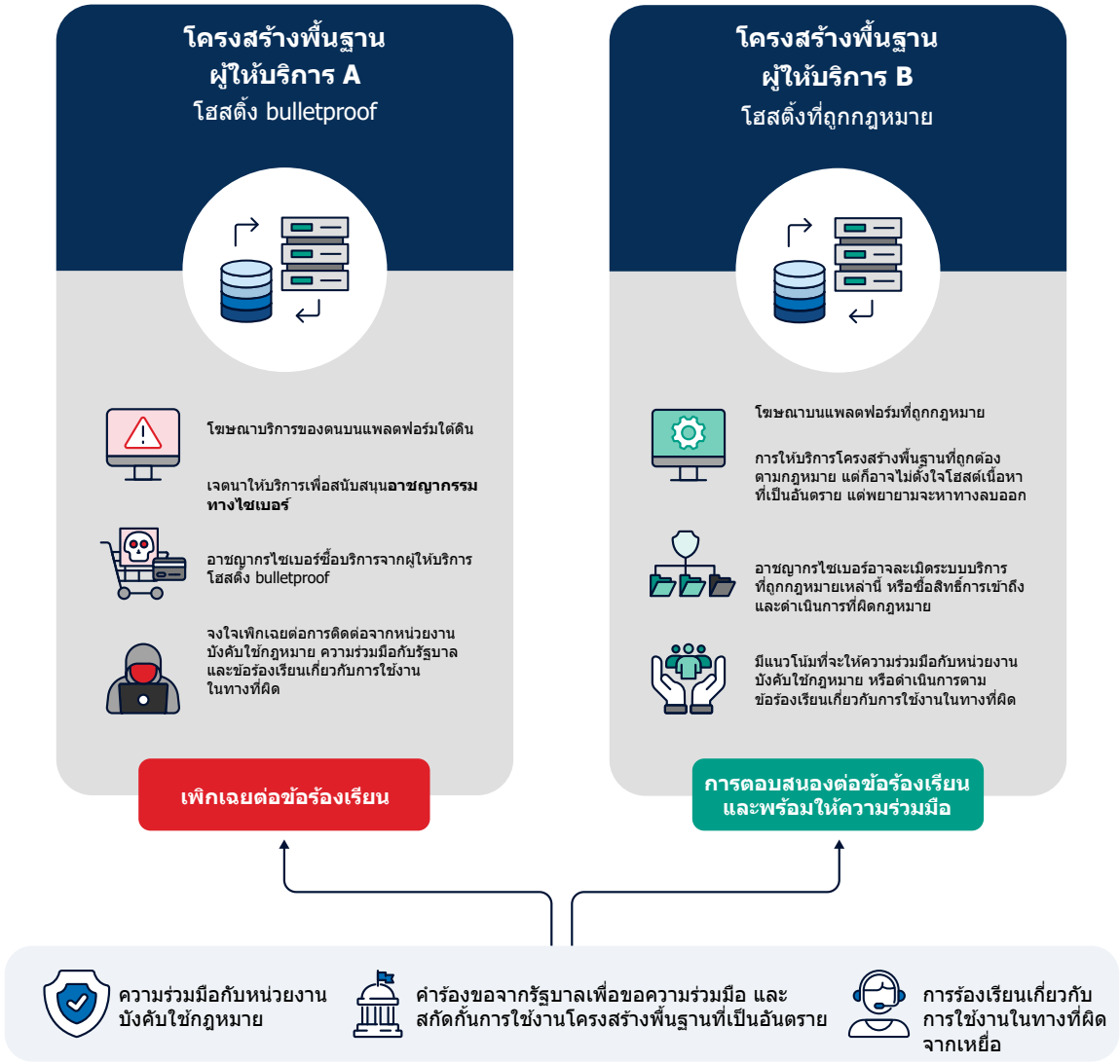
ตัวอย่างการนำเสนอโฆษณาของผู้ให้บริการ
โฮสติ้ง bulletproof ในเว็บบอร์ดใต้ดิน

ผู้ให้บริการ BPH ทำงานอย่างไร?

รูปแบบธุรกิจของผู้ให้บริการ BPH แต่ละรายจะแตกต่างกัน วิธีที่พบมากที่สุดคือการให้เช่าที่อยู่ IP แก่ลูกค้าที่เป็นอาชญากรไซเบอร์ และใช้วิธีการสลับเครือข่ายที่ซับซ้อนเพื่อช่วยปกปิดตำแหน่งที่ตั้ง ตัวตน และกิจกรรมของลูกค้า ในหลายกรณี ผู้ให้บริการ BPH จะขายต่อหรือให้เช่าที่อยู่ IP และเซิร์ฟเวอร์จากผู้ให้บริการโฮสติ้ง ศูนย์ข้อมูล หรือผู้ให้บริการอินเทอร์เน็ต (ISP) ที่ถูกต้องตามกฎหมายรายอื่น โดยที่ผู้ให้บริการ 'ต้นทาง (upstream)' เหล่านี้อาจไม่ทราบเลยว่าตนกำลังให้บริการโครงสร้างพื้นฐานแก่ผู้ให้บริการ BPH ซึ่งจากนั้นให้บริการ 'ปลายทาง (downstream)' ต่อไปยังอาชญากรไซเบอร์

ผู้ให้บริการ BPH มักตั้งค่าเครือข่ายและสถาปัตยกรรมระบบของตนเพื่อให้ยากต่อการระบุตัวตนของลูกค้า ตัวอย่างเช่น พวกเขามักจะเปลี่ยนแปลงข้อมูลระบุตัวตนที่เชื่อมต่อกับอินเทอร์เน็ตที่เกี่ยวข้องกับกิจกรรมของลูกค้าอยู่บ่อยครั้ง เช่น ที่อยู่ IP และชื่อโดเมนที่กำหนด เป็นต้น เทคนิคดังกล่าวท้าทายผู้ปกป้องและผู้สืบสวน ด้วยการทำให้ยากต่อการเชื่อมโยงเหตุการณ์กับที่อยู่ IP ที่ผู้กระทำความผิดหรือลูกค้าใช้ในเวลาใดก็ตาม นอกจากนี้ ผู้ให้บริการ BPH มักใช้โครงสร้างพื้นฐานในประเทศที่มีระบอบไซเบอร์ที่หละหลวม โดยที่ไม่มีมาตรการที่เป็นทางการในการตรวจสอบและป้องกันกิจกรรมทางไซเบอร์ที่เป็นอันตรายหรือมีมาตรการแต่หย่อนยานเกินไป

ผู้ให้บริการโฮสติ้ง bulletproof แตกต่างจาก
ผู้ให้บริการโครงสร้างพื้นฐานที่ถูกต้องตามกฎหมายอย่างไร?



การจัดการกับผู้ให้บริการ BPH ส่งผลกระทบต่อภัยคุกคามจากอาชญากรรมทางไซเบอร์อย่างไร

ผู้ให้บริการ BPH ถือเป็นยุทธศาสตร์สำคัญที่สามารถใช้เพื่อสกัดกั้นอาชญากรไซเบอร์ได้นับร้อยนับพันรายได้ในคราวเดียว อาชญากรไซเบอร์และผู้ไม่ประสงค์ดีในโลกไซเบอร์จำนวนมากใช้บริการเหล่านี้เพื่อให้การกระทำผิดของตนง่ายขึ้น โดยเชื่อว่ากิจกรรมของตนจะยังคงถูกปกปิดและสามารถดำเนินการต่อไปได้ แม้ว่าจะมีคำร้องขอให้ลบเนื้อหาหรือข้อร้องเรียนเกี่ยวกับการใช้งานในทางที่ผิดก็ตาม

อย่างไรก็ตาม หน่วยงานบังคับใช้กฎหมาย หน่วยงานของรัฐ และภาคเอกชน กำลังร่วมมือกันเพื่อจัดการและสกัดกั้นผู้ให้บริการโครงสร้างพื้นฐานผิดกฎหมายเหล่านี้ รวมถึงการใช้มาตรการป้องกัน เช่น การบล็อกการรับส่งข้อมูลทางอินเทอร์เน็ตจากผู้ให้บริการ BPH ที่เป็นที่รู้จักโดยตรง เป็นต้น กิจกรรมเหล่านี้ช่วยลดปริมาณอาชญากรรมทางไซเบอร์ที่เกิดขึ้นกับเครือข่ายของออสเตรเลียและเครือข่ายพันธมิตร และยังรวมถึงผู้ให้บริการโครงสร้างพื้นฐาน ‘ต้นทาง (upstream)’ และ ISP ที่ถูกกฎหมายที่อาจเอื้อโอกาสให้ผู้ให้บริการ BPH เข้าถึงอินเทอร์เน็ตและจัดเตรียมโครงสร้างพื้นฐานที่ปลอดภัยให้กับอาชญากรไซเบอร์โดยไม่รู้ตัว’

ผู้ให้บริการ BPH ไม่ใช่ผู้ให้บริการโครงสร้างพื้นฐานประเภทเดียวภายในระบบนิเวศของอาชญากรรมทางไซเบอร์ในรูปแบบการให้บริการ บริการเหล่านี้ช่วยให้ภัยคุกคามทางอาชญากรรมทางไซเบอร์ในออสเตรเลียดำเนินต่อไปได้อย่างต่อเนื่อง โดยการสนับสนุนแผนและกิจกรรมของอาชญากรไซเบอร์อย่างเปิดเผย และจงใจขัดขวางการสืบสวนและการตอบสนองตามกฎหมาย การดำเนินการกับผู้ให้บริการ BPH จึงเป็นการเผยให้เห็นถึงจุดอ่อนของบริการเหล่านี้ และของผู้ไม่ประสงค์ดีในโลกไซเบอร์ที่ใช้บริการเหล่านี้