บทความประชาสัมพันธ์

รู้เขา รู้เรา จัดระเบียบบ็อทส์ดีและร้ายให้อยู่หมัด

เป็นเรื่องยากที่เราจะก้าวผ่านวงจรข่าวใดๆ โดยไม่มีบ็อทส์เข้ามามีส่วนร่วมด้วย ไม่ว่าจะเป็นการปล่อยสแปม เผยแพร่ข่าวลวง หรือ การสร้างโปรไฟล์ปลอม รวมถึงเนื้อหาบนโซเชียลมีเดียบ่อยครั้งล้วนมีอิทธิพลต่อความคิดเห็นสาธารณะ อาจจะก่อให้เกิดกระแสการประท้วง หรือแม้แต่การปะทุอารมณ์ให้คุกรุ่นในการเลือกตั้ง

การดีเบตในระหว่างการเลือกประธานาธิบดีสหรัฐในปี 2016 บ็อทส์ ได้ถูกนำมาใช้ในทวิตเตอร์ เพื่อโปรโมทให้หนึ่งในผู้ลงสมัครสร้างแต้มต่อให้เหนือกว่าผู้สมัครรายอื่น ด้วยสัดส่วน 7:1.1 ปัจจุบัน การเลือกตั้งประธานาธิบดี ในปี 2020 ที่ยังเหลือเวลาอีกสองปีนั้น การป่วนจากพวกเกรียนคีย์บอร์ดทั้งหลายก็ยังคงมีอยู่อย่างมากมาย ล่าสุดในช่วง 30 วัน เกิดทวิตด้านลบ ประมาณ 2% ถึง 15% ที่เกี่ยวข้องกับผู้สมัครลงเลือกตั้งที่ได้ประกาศตัว ในการแข่งขันชิงตำแหน่งเก้าอี้ประธานาธิบดีของปี 2020 ที่สามารถตามรอยกลับไปที่บัญชีบ็อทส์และขยายไปยังบ็อทส์อื่นได้ออกเป็นวงกว้าง

อะไรคือบ็อทส์? บ็อทส์เป็นคำเรียกสั้นๆ ของคำว่า" โรบ็อทส์" เป็นโปรแกรมซอฟต์แวร์ ที่ทำงานอัตโนมัติ (สคริปท์) บนอินเทอร์เน็ต ต้นกำเนิดถูกออกแบบมาให้ทำงานอย่างง่ายๆ ธรรมดา และเป็นงานบนเว็บที่คนไม่นิยมทำเพราะต้องทำซ้ำๆ หรือเป็นงานที่ไม่สามารถทำได้รวดเร็วพอ และเหนือไปกว่าการทำงานแบบอัตโนมัติ บ่อยครั้ง บ็อทส์ยุคใหม่ยังได้รับการออกแบบมาเพื่อให้จำลองพฤติกรรมของมนุษย์ด้วย ขึ้นอยู่กับตัวคุณล้วนๆ ว่าเชื่อใจตัวเลขไหนเป็นพิเศษ มีการคาดการณ์ว่าบ็อทส์ทุกประเภทคิดเป็นสัดส่วนสูงถึง 21% และมากกว่า 50% ของปริมาณการใช้อินเทอร์เน็ตในปัจจุบัน

แมรี่ มีเกอร์ อดีตนักวิเคราะห์ด้านความปลอดภัยของหลักทรัพย์วอลส์สตรีท ระบุว่า ปริมาณการใช้อินเทอร์เน็ตที่สร้างจากบ็อทส์ทั่วโลกสูงกว่าปริมาณของข้อมูลที่มนุษย์สร้างขึ้นในปี 2559 เสียอีก
ในเดือนธันวาคม ปี 2018 เดอะวอลล์สตรีท เจอร์นัล อ้างข้อมูลจาก อะโดบี ว่า "ราว 28% ของปริมาณการเข้าชมเว็บไซต์นั้นมาจากบ็อทส์ และสัญญาณอะไรก็ตามที่ไม่ใช่มนุษย์"

ในปี 2017 ทวิตเตอร์ คาดการณ์ว่า อาจมีบัญชีชื่อหรือแอคเคาท์ของทวิตเตอร์สูงถึง 48 ล้านบัญชี ซึ่งคิดเป็น 15% ของจำนวนผู้ใช้ทั้งหมด เป็นบ็อทส์ ไม่ใช่คนจริงๆ

ตามข้อมูลจากเวอริซอน 77% จากรายงานช่องโหว่บนเว็บแอพพลิเคชั่น ในปี 2016 เกิดจากบ็อทส์เน็ท ดังนั้น เราจะก้าวผ่านสถานการณ์ที่เกิดจากฝีมือบ็อทส์ได้อย่างไร? พวกนั้นมีหน้าที่เพียงแค่สร้างปัญหาบนอินเทอร์เน็ต หรือก่อให้เกิดความเสียหายทางธุรกิจ การเมืองและสังคมเท่านั้นหรือ? แล้วพวกบ็อทส์นั้นเคยทำอะไรดีๆ บ้างหรือเปล่า?

นี่คืออรรถาธิบายทั้งเรื่องดี เรื่องร้าย และเรื่องน่าชังของบ็อทส์ และเรายังมีแผนการณ์ที่ชัดเจนในการพิชิตบ็อทส์ร้ายให้ออกจากเครือข่ายของเราด้วย

เมื่อบ็อทส์ "ดี"

บ็อทส์ “ดี” ได้รับการออกแบบมาเพื่อช่วยเหลือด้านธุรกิจและผู้บริโภค ถือกำเนิดขึ้นมาตั้งแต่ต้นยุค 1990 เมื่อครั้งเครื่องมือค้นหาหรือเสิรชเอ็นจิ้นที่เป็นบ็อทส์ได้รับการพัฒนาเพื่อสืบเสาะไปตามอินเทอร์เน็ต ไม่ว่าจะเป็น กูเกิล ยาฮู และบิง เสิชเอ็นจิ้นเหล่านี้จะไม่สามารถเกิดขึ้นได้หากไม่มีบ็อทส์ ตัวอย่างอื่น ๆ ของบ็อทส์ที่ดีซึ่งส่วนใหญ่มุ่งเน้นไปที่ผู้บริโภค รวมถึง:

แชทบ็อทส์ (เช่น แชทเตอร์บ็อทส์, สมาร์ทบ็อทส์, ทอล์คบ็อทส์, ไอเอ็มบ็อทส์, โซเชียลบ็อทส์, คอนเวอร์เซชั่นบอทส์) โต้ตอบกับมนุษย์ผ่านข้อความหรือเสียง หนึ่งในข้อความแรกที่ใช้คือ การบริการลูกค้าออนไลน์ และแอพส่งข้อความเช่น เฟสบุ๊ค เมสเซ็นเจอร์ และ ไอโฟนเมสเสจ

สิริ (Siri) **คอร์ทานา** (Cortana) และ**อเล็กซา** (Alexa) ล้วนเป็นแชทบ็อทส์ แต่ก็เป็นโมบายแอพที่ให้คุณสามารถสั่งซื้อกาแฟ และแจ้งกลับเมื่อทำเสร็จได้ นอกจากนี้คุณยังสามารถดูตัวอย่างภาพยนตร์ และค้นหาเวลาฉายภาพยนต์ในพื้นที่ใกล้ๆ หรือช่วยส่งภาพของรุ่นรถยนต์ และทะเบียนรถเมื่อคุณต้องการใช้บริการรถโดยสารด้วยช้อปบ็อทส์ สืบค้นไปในอินเทอร์เน็ตเพื่อค้นหาสินค้าที่ต้องการในราคาต่ำสุด การเฝ้าติดตามบ็อทส์เพื่อเช็คสภาพ (พร้อมให้บริการและมีการตอบสนอง) ของเว็บไซต์ Downdetector.com เป็นตัวอย่างของเว็บไซต์อิสระ ที่ให้ข้อมูลสถานะแบบเรียลไทม์ รวมถึงกรณีเว็บล่ม และบริการอื่นๆ

เมื่อบ็อทส์ “ร้าย”

ประวัติศาสตร์ ได้ทำให้เราเรียนรู้ว่า อะไรก็ตามที่ออกแบบมาเพื่อทำในสิ่งที่เป็นประโยชน์ได้ ก็สามารถถูกนำมาใช้ในทางที่ไม่ดีได้เช่นกัน และนี่เป็นสิ่งที่เกิดขึ้นจริงของบ็อทส์ บ็อทส์ “ตัวร้าย” เป็นที่แพร่หลาย เพราะมันถูกสร้างได้อย่างง่ายดาย โดยใครก็ได้ แม้แต่เด็กที่มีอายุเพียง 13 ปีก็สามารถเขียนโปรแกรมพื้นฐาน หรือเขียนโปรแกรมซื้อขายได้ด้วยการจ่ายเงินเพียงเล็กน้อยเท่านั้น

คุณสามารถซื้อบ็อทส์ เพื่อมาเพิ่มเรตติ้งผลิตภัณฑ์ หรือ จ้อโกงโฆษณา ด้วยเงินเพียง 2 ดอลล่าร์สหรัฐ คุณสามารถซื้อคนติดตามทวิตเตอร์ 5,000 คนด้วยเงินไม่ถึง 50.10 ดอลล่าร์สหรัฐ และคุณไม่จำเป็นต้องไปที่เว็บมืดเพื่อซื้อบ็อทส์อีกต่อไป : เพราะมีโฆษณาหลายประเภทถูกขายบนอินสตาแกรมแล้วด้วย

สำหรับเหล่าแฮคเกอร์ พลังของบ็อทส์ที่แท้จริงถูกควบรวมอยู่ในบ็อทเน็ท นั่นคืออุปกรณ์ที่ติดเชื้อมัลแวร์ (ซอมบี้) จำนวนมหาศาล มัลแวร์ที่ถูกโปรแกรมมาให้ปฏิบัติการตามคำสั่งของคนโจมตี หรือ ผู้เลี้ยงบ็อทนั่นเอง

บ็อทเน็ทส์ จะสะสมพลังประมวลผลที่จำเป็นในการโจมตีครั้งใหญ่ จากเซิร์ฟเวอร์ที่ใช้ออกคำสั่งและควบคุม บ็อทส์จะส่งคำสั่งตรงถึงซอมบี้ว่าต้องทำอะไรบ้าง

อุปกรณ์ประมวลผลแบบเสมือนทั้งหมดนั้น ถูกยึดโดยบ็อทส์ร้าย เพื่อใช้ในกิจกรรมประสงค์ร้ายที่หลากหลายเจตนา ตามที่ระบุไว้ด้านล่าง (หมายเหตุ: ไม่มีอะไรบอกว่าอะไรคือสิ่งที่ “ถูก” หรือ วิธีมาตรฐานในการจัดหมวดหมู่บ็อทส์ หรือแบ่งประเภทตามพฤติกรรมของบ็อทส์ แต่นี่เป็นการจัดกลุ่มตามเป้าประสงค์ ของบทความนี้)

- **การโจมตีแบบดีดอส** (Distributed denial-of-service :DDoS) การโจมตีเป้าหมายแบบพร้อมๆ กัน เพื่อทำให้ไม่สามารถให้บริการได้ โดยผู้โจมตีจะใช้บ็อทเน็ทส์ เพื่อทำลายแอพลิเคชั่น หรือช่องโหว่ในเครือข่าย ในช่วงต้นปี 2000 บ็อทเน็ทส์จะประกอบด้วย พีซีที่ติดเชื้อ และใช้การโจมตี ดีดอสที่ประสบผลสำเร็จ ใน Yahoo, Amazon.com, CNN, E*TRADE, และ eBay ปัจจุบัน บ็อทเน็ทส์ ดีดอส ถูกสร้างเพื่อให้ติดอุปกรณ์บน

อินเทอร์เน็ต ออฟธิงส์ (IoT) มากกว่าอยู่บนเครื่องพีซี ด้วยช่องโหว่หลายพันล้านที่เขียนในอุปกรณ์ IoT ที่อยู่ในตลาด ทำให้ผู้โจมตีสามารถสร้างบ็อทเน็ทส์จำนวนมหาศาล (thingbots) เพื่อใช้ในการโจมตีแบบดีดอส DDoS (สูงสุดถึง 1 เทราไบท์ต่อวินาที) เช่นเดียวกับที่เริ่มครั้งแรกในปี 2016 Mirai ที่ใช้โจมตีบนระบบความปลอดภัย Krebs Dyn และ OVH และในปี 2018 ที่มีการโจมตี ระดับ 1.3 เทราไบท์ต่อวินาทีบน GitHub (แลป F5 รายงานอย่างกว้างขวางเกี่ยวกับภัยคุกคามอย่างต่อเนื่องของการโจมตี ธิงค์บ็อทส์ และการขยายขอบเขต นอกเหนือจาก DDoS ไปยังสกุลเงินดิจิตัลอย่างคริปโตเคอร์เรนซี่ การเก็บข้อมูลที่ใช้ยืนยันตัวตน และการโจมตีทุกช่องทางใน การพิสูจน์ตัวตน ไม่ว่าจะเป็นคลังการรวบรวมข้อมูลประจำตัวที่ถูกบรรจุไว้ในข้อมูลประจำตัว credential stuffing)

- **ข้อมูลประจำตัว** การใช้ประโยชน์จากการยืนยันตัวตนในบัญชีชื่อที่ถูกขโมยมาหลายพันล้านบัญชี แฮคเกอร์ใช้บ็อทส์ เพื่อปล่อยการโจมตีแบบอัตโนมัติโดย “นำชื่อผู้ใช้และรหัสผ่าน ที่ถูกขโมยมารวมกัน” เพื่อล็อกอินเข้าเพจของเว็บไซต์ต่างๆ เป้าหมายสูงสุดคือ การเข้าควบคุมแอคเคาท์ และเนื่องจากมีคนมากมายที่ใช้รหัสยืนยันตัวตนชุดเดียวกันหลายๆ แอคเคาท์ อัตราความสำเร็จ และความคุ้มค่าสำหรับแฮคเกอร์จึงมีสูงมาก

- **การฉ้อโกงกิฟท์และเครดิตการ์ด** ผู้โจมตี ใช้บ็อทส์ เพื่อเจาะในแอคเคาท์กิฟท์การ์ด เพื่อหาข้อมูลที่ใช้ยืนยันตัวตน เครเดนเชี่ยล/credentials หลังจากนั้นจะสร้างการ์ดปลอม และขโมยมูลค่าเงินสดในการ์ด

  ในกรณีของบัตรเครดิต ผู้โจมตีจะใช้บ็อทส์ ทดสอบการพิสูจน์ตัวตนของบัตรเครดิตที่ขโมยมา ด้วยธุรกรรมที่มีมูลค่าน้อยก่อน (เช่น หนึ่งดอลล่าร์สหรัฐ) จากนั้นเมื่อสำเร็จ แฮคเกอร์ จะใช้การยืนยันตัวตนที่ขโมยมา เพื่อซื้อสินค้าหรือบริการในครั้งใหญ่ขึ้น หรือถอนเงินสดออกจนหมดบัญชี

- **สแปม** จะเกี่ยวข้องกับ พฤติกรรมทุกประเภทที่ไม่ต้องการ “สแปม” เช่นการส่งอินบ็อกซ์ ด้วยอีเมลที่ไม่ต้องการ ซึ่งมีลิงค์ประสงค์ร้าย เขียนการรีวิวสินค้าปลอม การสร้างบัญชีโซเชียลมีเดียปลอม เพื่อเขียนคอนเท้นท์ปลอม หรือสร้างอคติให้เกิด การเพิ่มเพจวิว (เช่น วิดีโอ YouTube) หรือผู้ติดตาม (เช่นบนทวิตเตอร์หรืออินสตราแกรม) การเขียนคอมเม้นท์บนฟอรัม หรือไซต์โซเชียลมีเดียทำให้เกิดการโต้เถียง การล็อกผลคะแนนหรือโกงการเลือกตั้ง เป็นต้น

- **การป้องกันเนื้อหาจากการดูดเวบ** รวมถึง แฮคเกอร์ที่สแกน หรือดึง (ขโมย) ลิขสิทธิ์ หรือข้อมูลเครื่องหมายการค้า จากเว็บไซต์ และ จัดเก็บในเครื่องของตนเอง และจากนั้นนำกลับมาใช้ใหม่ – บ่อยครั้งจุดประสงค์เพื่อการแข่งขัน - ในเว็บของตนเอง

- **การดูดข้อมูล** ได้แก่ ทรัพย์สินทางปัญญา ข้อมูลผลิตภัณฑ์ และราคาของผลิตภัณฑ์ สายการบิน โรงพยาบาล เกมออนไลน์ และเว็บไซต์จองตั๋ว มักจะมีช่องโหว่ให้กับนักดูดเว็บได้เสมอ

- **การโกงคลิ๊ก** โดยมาก จะเกี่ยวข้องกับการโกงค่าโฆษณา การฉ้อโกงนั้นเป็นบ็อท ไม่ใช่คน ที่จะคลิ๊กในโฆษณา และไม่มีเจตนาจะซื้อผลิตภัณฑ์หรือบริการที่โฆษณานั้น แต่เป้าหมายคือเร่งเพิ่มรายได้ให้กับเจ้าของเว็บ (หรือคนโกงรายอื่น) ที่จะได้รับเงินตามจำนวนการคลิ๊กโฆษณานั่นเอง บ็อทส์ลักษณะนี้จะรายงานข้อมูลที่บิดเบือน และคิดค่าใช้จ่ายสูง เนื่องจากต้องจ่ายให้กับการคลิ๊กที่ไม่ได้เกิดจากมนุษย์ และยิ่งเลวร้ายไปอีก บริษัทเหล่านั้นไม่ได้รายได้จาก “นักช้อปลวง” การโกงคลิ๊ก จะถูกนำมาใช้โดยบริษัทที่มีเจตนาสร้างค่าใช้จ่ายด้านโฆษณาให้กับคู่แข่ง

- **การขัดขวางการประมูล** จะเกิดขึ้นในเว็บไซต์ประมูล เมื่อตัวร้ายมาเยือนในเวลาที่เหมาะสม การประมูลผลิตภัณฑ์หรือบริการในนาทีสุดท้าย เพื่อไม่ให้มีคนประมูลได้
- **ความชาญฉลาดที่จะเก็บเกี่ยวจากการสแกนเว็บเพจ** ฟอรัมอินเทอร์เน็ต โซเชียลมีเดีย และเนื้อหาอื่นๆ เพื่อหาอีเมลที่ถูกต้อง และข้อมูลอื่น ที่ผู้โจมตี จะสามารถใช้เพื่อส่งสแปมเมล หรือทำแคมเปญโกงโฆษณา

ทำไมจึงต้องให้ความใส่ใจ

บ็อทส์ร้าย สร้างความเสียหายให้กับองค์กรและโลกของอินเทอร์เน็ต บรรดาตัวที่ปล่อยการโจมตี DDoS(โดยเฉพาะอย่างยิ่งที่บุกเวบแอพลิเคชั่น) สามารถทำลายล้าง จากการประมวลผลมหาศาลที่บ็อทเน็ทส์ครอบครองอยู่ และบริษัทส่วนใหญ่จะเริ่มไม่สามารถจัดการการโจมตีได้ด้วยตนเองเมื่อมีการโจมตีที่ใช้ความเร็วระดับ 300 – 500 กิกะบิทต่อวินาทีและต่ำกว่าหนึ่งเทราบิทต่อวินาที และค่าใช้จ่ายอาจมากเท่าการทำลายที่เกิดขึ้น ในการสำรวจบุคลากรมืออาชีพด้านซีเคียวริตี้ปี 2017 ประมาณ 75% ของการโจมตีแบบ DDoS อาจทำให้บริษัทมีความเสียหาย ตั้งแต่ 500,000 ดอลล่าร์สหรัฐ จนถึง 10 ล้านดอลล่าร์สหรัฐ และบ็อทส์ร้าย ยังสร้างความเสียหายให้กับบริษัทในหลายทางมากกว่าด้านการเงิน สามารถสร้างทราฟฟิคเพิ่มในเครือข่าย ที่ทำให้เวบไซต์ทำงานทราฟฟิคช้าลง และทำให้เราต้องจ่ายค่าแบนด์วิธ และคลาวด์ที่เพิ่มขึ้น

บ็อทส์สามารถทำให้ทราฟฟิคออกจากเว็บไซต์ ฉกฉวยโอกาสที่จะสร้างรายได้จากคุณ และอาจสามารถสร้างค่าใช้จ่ายมหาศาล ถูกคิดค่าใช้จ่ายโฆษณาปลอม และอาจทำลายชื่อเสียงของบริษัทจากข่าวลวง รีวิวที่เลวร้าย และกลยุทธ์ที่ซ่อนเร้น และเนื่องด้วยบ็อทส์ในปัจจุบัน เก่งในการซ่อนตัว และปรากฏให้ดูเหมือนดีต่อหน้าผู้ใช้ นั่นทำให้การตรวจจับยากขึ้นไปอีก

เมื่อเส้นทางของบ็อทร้ายที่ไม่มีจุดสิ้นสุด

เหรียญมีสองด้านเสมอ ก็เหมือนกับบ็อทส์ที่มีทั้งด้านดีและร้าย สุดแต่ว่าผู้ใช้จะเจตนาให้เห็นในด้านไหน เช่น Selenium ที่ออกแบบมาเพื่อใช้เฟรมเวิร์คทสอบซอฟต์แวร์ที่พกพาได้สำหรับเว็บแอพ แต่สามารถนำมาใช้เป็นเครื่องมือการดูดข้อมูลเว็บหรือสร้างบ็อท เครื่องมือในการสแกนยอดนิยม อย่าง Shodan และ Shadow Security Scanner จะถูกนำมาใช้เพื่อการวิจัย แต่ก็สามารถถูกแฮคเกอร์ นำมาใช้โจมตีข้อมูลเป้าหมายได้เช่นกัน

กำจัดอย่างไร

ไม่มีโซลูชั่นใดโซลูชั่นหนึ่ง ที่จะกำจัดเหล่าบ็อทส์ร้ายออกจากเครือข่ายได้ แต่ก็มีวิธีการที่มีประสิทธิผลที่จะป้องกันได้ รูปแบบคล้ายการต่อจิ๊กซอว์ โดยคุณสามารถเก็บรวบรวมอัตลักษณ์หรือพฤติกรรมที่มีรูปแบบที่หลากหลาย แล้วนำมาประมวลผลก่อให้เกิดภาพรวมที่จับต้องได้

นี่เป็นบางส่วนที่ควรพิจารณาเพื่อไขปริศนาปัญหาด้านความปลอดภัยจากบ็อทส์

- **ตรวจสอบย้อนกลับ** มองหาแหล่งที่มาของไอพีแอดเดรส ที่โดยมากจะไม่มีประสิทธิภาพ สำหรับตรวจจับบ็อทส์ร้าย เนื่องจากแฮคเกอร์ บ่อยครั้งจะปล่อยไอพีหลายร้อยแอดเดรสที่แตกต่างกัน เพื่อเลี่ยงต่อการถูกสงสัย แต่การตรวจสอบย้อนกลับ จะมีวิธีที่มีประสิทธิภาพที่ใช้ระบุบ็อทส์ที่ดีได้ เช่นทราฟฟิคจากเสิร์ชเอ็นจิน

ไอพีแอดเดรส์เหล่านี้ จะอยู่ในบัญชีซื่อที่ดี และจงจำไว้ว่าบัญชีเหล่านี้ต้องอัพเดทเป็นประจำ เพื่อให้ได้ประสิทธิผล

- **การตรวจจับอัตลักษณ์ (ซิกเนเจอร์ บ็อทส์)** สามารถระบุได้จากอัตลักษณ์ลักษณะเฉพาะหรือ รูปแบบเฉพาะที่สามารถสังเกตได้จากอดีต การตรวจจับบ็อทส์จากอัตลักษณ์มีความเสี่ยงต่ำ และเชื่อถือได้ แต่ก็ไม่สามารถตรวจจับบ็อทใหม่หรือที่ไม่รู้จักมาก่อนได้ การติดตามบ็อทส์ใหม่ คุณต้องอัพเดทอัตลักษณ์ของบ็อทส์ที่รู้จัก และสร้างใหม่ โดยใช้การวิเคราะห์จากทราฟฟิคที่รวบรวมได้
- **การตรวจจับบ็อทส์โดยดูจากรูปแบบของพฤติกรรม** รวมถึงการมองหาพฤติกรรมที่ชวนสงสัย เช่น ปริมาณทราฟิคสูงหรือผิดปกติ การเปิดพอร์ทที่ไม่ได้มาตรฐาน ความพยายามที่จะเริ่มหรือหยุดโพรเซส ความพยายามดาว์นโหลดให้ไฟล์ทำงานหรือเข้าถึงไฟล์ที่หวงห้าม และรูปแบบการท่องเน็ตแบบที่ใช้หุ่นยนต์ ทั้งหมดล้วนเป็นสัญญาณของกิจกรรมที่เกิดจากบ็อทส์ทั้งสิ้น
- **ตรวจสอบบราวเซอร์เพื่อหาเอเย่นต์ผู้ใช้ปลอมและส่วนขยายบราวเซอร์ประสงค์ร้าย**

  ทุกบราวเซอร์จะมีอัตลักษณ์เป็นของตัวเองเพื่อที่จะระบุได้ว่าสร้างมาอย่างไร รวมถึงการใช้คอนฟิก หรือการติดตั้งในอุปกรณ์ ส่วนหนึ่งของอัตลักษณ์ รวมถึงเอเย่นต์ผู้ใช้ ที่ระบุชื่อ และเวอร์ชั่นของบราวเซอร์ที่เฉพาะเจาะจง และระบบปฏิบัติการ ทว่าวิ่งนี้ และข้อมูลอื่นๆ สามารถปลอมแปลงด้วยความเชี่ยวชาญของผู้โจมตี ส่วนต่อขยายบราวเซอร์ที่ต้องสงสัยก็อาจเป็นสัญญาณของบ็อทส์ได้เช่นกัน บ็อทที่มีอยู่จำนวนมาก ถูกออกแบบเพื่อให้ดูดข้อมูลในเว็บ รวมถึงการปล่อยตัวประสงค์ร้ายแบบอื่นๆ อัตลักษณ์ที่ปรากฏแบบไม่มีเหตุผลควรจะให้คะแนนความเป็นไปได้ว่าเป็นบ็อทส์
- **ใช้** CAPTCHAs เพื่อแยก มนุษย์ จากพฤติกรรมของบ็อท บนเว็บไซต์ นี่อาจเป็นวิธีที่พิสูจน์ได้ไม่ทั้งหมด แต่ก็เพียงพอจะช่วยบล็อกทราฟฟิคบางส่วน
- **ใช้** JavaScript challenge เพื่อตรวจสอบ ว่าบราวเซอร์ปกติได้นำมาใช้ บ็อทส์เกือบทั้งหมด จะไม่สามารถตอบสนองต่อ JavaScript challenge ดังนั้นหาบราวเซอร์ โต้ตอบกลับมา ทราฟฟิคนั้น ก็เป็นไปได้ว่าจะไม่ใช่บ็อทส์
- การนำบ็อทส์ดีมาใช้ เช่น เสิร์ชเอ็นจิน เพื่อลดการโหลดในเว็บไซต์ลง บ็อทส์ดี สามารถทำงานโดยใช้ปริมาณแบนด์วิธระดับกลางได้
- **การจำกัดเพดานอัตราทราฟฟิคที่ต้องสงสัย** หากไม่มั่นใจว่าเป็นทราฟิคของบ็อทส์หรือไม่ นี่จะช่วยสามารถรักษาทราฟิคที่ดี ให้ไหลเวียนในเว็บไซต์ระหว่างที่คุณกำลังตรวจสอบต่อมา เช่น ทราฟฟิคที่เพิ่มนั้น มาจากไอพีแอดเดรสเฉพาะนั้น ถูกต้อง หรือมีความเป็นไปได้ว่าเป็นการโจมตีที่ใช้ credential stuffing หรือเป็นการละเมิดรหัสผ่านของผู้ใช้นั่นเอง
- **ตัด" โอกาส" การโจมตี** หมายถึง การมองหาระบบที่รันแอพลิเคชั่นเฉพาะ เช่น Outlook Web Access (OWA) หากองค์กรของคุณไม่ได้ใช้ OWA คุณสามารถสร้างการรบกวน และโหลดบนเครือข่ายให้น้อยลง โดยบล็อคทราฟฟิคอัตโนมัติใดๆ ที่เราไม่รู้จัก

- **ให้คะแนนระดับความเสี่ยงตามเซสชั่น** โดยใช้การผสมผสานหลากวิธีที่ได้กล่าวมา เพื่อเพิ่มเติม หรือ ลบจุดคะแนนความเสี่ยง จากนั้นจะทำให้คุณตัดสินใจได้ว่าเมื่อใดและแอคชั่นประเภทใด ที่คุณต้องการในการต้านความเสี่ยงในอุปกรณ์ปลายทาง

น่าจะเป็นประโยชน์มาก หากจะทราบว่าวิธีการใดที่ไม่สามารถกำจัดบ็อทส์ร้ายอย่างไม่มีประสิทธิภาพ เช่น การใช้ geofencing ในอดีตคุณสามารถหยุดบ็อทส์จำนวนมากโดยบล็อกทราฟฟิคที่มาจากประเทศที่ทราบดีว่า ปล่อยการโจมตี แต่ปัจจุบันแฮคเกอร์ ก้าวล้ำไปกว่านั้น พวกเขาปล่อยการโจมตีจากหลายร้อยไอพีไอเดรสและกระจายไปทั่วทุกภูมิภาค

นอกจากนี้ในหลายบริษัท มีลูกค้า คู่ค้า และการรับส่งข้อมูลที่ถูกกฎหมายอื่น ๆ ที่มาจากประเทศที่เฉพาะเจาะจง ดังนั้นจึงมักจะไม่สามารถปิดกั้นการรับส่งข้อมูลทั้งหมดจากที่ตั้งที่เฉพาะเจาะจง ในขณะที่ geofencing ซึ่งเป็นการระบุตำแหน่งพิกัดว่าอุปกรณ์เข้าออกจากที่ใด ยังคงมีอยู่ในกล่องเครื่องมือรักษาความปลอดภัยของคุณ แต่ด้วยสถานะของตัวมันเองในตอนนี้ ยังไม่ใช่เครื่องมือที่ดีที่สุดในการต่อสู้กับบ็อทส์

บทสรุป

ทั้งบ็อทส์ดีและร้าย คิดเป็นสัดส่วนสูงถึง กว่า 50% ของปริมาณการใช้อินเทอร์เน็ต จำเป็นอย่างยิ่งสำหรับองค์กรที่ควรตระหนักรู้ว่าแนวโน้มนี้กำลังเพิ่มขึ้น แฮคเกอร์ที่ชาญฉลาดประสบการณ์มาก จะยังคงพัฒนาบ็อทส์ที่อันตรายซับซ้อนและร้ายแรง โดยเฉพาะอย่างยิ่ง อุปกรณ์หลายพันล้านของอุปกรณ์ IoT ที่เขียนให้มีช่องโหว่ (โดยตั้งรหัสผ่านอัตโนมัติ และอินเทอร์เฟซที่ไม่ได้ติดตั้งมา) จนกว่าผู้ผลิตอุปกรณ์ IoT จะถูกบังคับใช้ด้วยกฎหมาย เพื่อสร้างความปลอดภัยให้กับอุปกรณ์ แฮคเกอร์ก็จะยังคงใช้เพื่อปล่อยการโจมตีแบบบวงกว้างและหลายมิติโดยเริ่มต้นจากบ็อทส์

ขณะเดียวกัน การพร้อมใช้ของบ็อทส์อย่างง่ายดายที่ให้ฟรี หรือการจ่ายในราคาต่ำๆ เพื่อให้เหล่า "มือสมัครเล่นที่หัดเขียนสคริปท์วัยละอ่อน" ในอินเทอร์เน็ตระบบเปิด ก็เป็นปัญหาที่เติบโตขึ้น เนื่องจากแม้จะเป็นบ็อทส์อย่างง่าย ที่มาจากคนไม่มีประสบการณ์ก็อาจเป็นอันตรายได้สูงเช่นเดียวกัน

คำแนะนำสำหรับองค์กรคืออะไร? เตรียมตัวคุณให้พร้อมรับมือการโจมตีของทราฟฟิคบอททุกประเภท ยกระดับการควบคุมความปลอดภัยในการจัดการบ็อทส์ดีได้อย่างเต็มประสิทธิภาพ และเก็บทราฟฟิคบ็อทส์ร้ายบนเครือข่ายให้มากที่สุดเท่าที่จะเป็นไปได้

- ใช้เว็บแอพลิเคชั่นไฟร์วอลล์ สำหรับตรวจจับบ็อทส์ทั้งหลาย โดยตรวจจับอัตลักษณ์สำคัญ signature-based และลักษณะพฤติกรรมที่มีรูปแบบ behavior-based ของบ็อทส์
- ใช้ CAPTCHAs
- ใช้ JavaScript challenges
- ให้เพดานคะแนนทราฟฟิคต้องสงสัย
- บล็อกทราฟิคที่ประเมินความเสี่ยงว่า "น่าจะใช่"

# # #