imperva

บริษัทในเครือ Thales

2024

# รายงาน Bad Bot

imperva
บริษัทในเครือ Thales

# รายงาน Bad Bot

ประจำปี 2024

## สารบัญ

# รายงาน Bad Bot ประจำปีครั้งที่ 11 ของ Imperva จะตรวจสอบและสืบสวนลักษณะของการเข้าเยี่ยมชมทางอินเทอร์เน็ตแบบอัตโนมัติ ซึ่งส่วนใหญ่เป็นการโจมตีด้วยบอทแบบอัตโนมัติ

การโจมตีดังกล่าวมีความซับซ้อนมากขึ้นทุกวัน โดยเลี่ยงวิธีการตรวจจับแบบเดิม ๆ และก่อให้เกิดความสับสนวุ่นวายบนอินเทอร์เน็ต รายงานการวิเคราะห์ข้อมูลที่รวบรวมจากเครือข่ายทั่วโลกของ Imperva ในปี 2023 รวมถึงคำขอของ Bad Bot ที่ถูกบล็อกเกือบ 6 ล้านล้านครั้งที่ไม่ระบุชื่อในโดเมนและอุตสาหกรรมหลายพันแห่ง

รายงานนี้มีวัตถุประสงค์เพื่อให้ข้อมูลที่สำคัญเกี่ยวกับลักษณะและผลกระทบของบอท เพื่อช่วยให้องค์กรเข้าใจถึงความเสี่ยงที่อาจเกิดขึ้นจากการเข้าเยี่ยมชมของบอทได้ดีขึ้น เมื่อไม่ได้รับการจัดการอย่างเพียงพอ

**รายงานมุ่งเน้นไปที่กิจกรรม Bad Bot ในเลเยอร์แอปพลิเคชันของโมเดล OSI (เลเยอร์ 7) กรณีการใช้งานบอทเหล่านี้แตกต่างอย่างสิ้นเชิงไปจากการโจมตี DDoS แบบปริมาณ ซึ่งเป็นการเล่นงานโปรโตคอลเครือข่ายระดับล่าง**

Bad Bot จะมีปฏิสัมพันธ์กับแอปพลิเคชันในลักษณะที่เลียนแบบผู้ใช้ที่ถูกต้อง ทำให้ตรวจจับและบล็อกได้ยากยิ่งขึ้น พวกเขาใช้ประโยชน์จากตรรกะทางธุรกิจโดยใช้ประโยชน์จากฟังก์ชันและกระบวนการตามจุดประสงค์ของแอปพลิเคชันมากกว่าช่องโหว่ทางเทคนิค Bad Bot ช่วยให้เกิดการละเมิด การใช้งานในทางที่ผิด และการโจมตีเว็บไซต์ แอปมือถือ และ API ได้อย่างรวดเร็ว โดยช่วยให้ผู้อยู่เบื้องหลังบอท ผู้โจมตี คู่แข่งที่เป็นศัตรู และผู้ฉ้อโกงสามารถทำกิจกรรมที่เป็นอันตรายได้

กิจกรรมต่าง ๆ เช่น การดูดข้อมูลจากเว็บ การทำเหมืองข้อมูลเพื่อแข่งขัน การเก็บเกี่ยวข้อมูลส่วนบุคคลและข้อมูลทางการเงิน การพยายามเข้าสู่ระบบโดยการบังคับ, Scalping, การฉ้อโกงโฆษณาดิจิทัล การโจมตีแบบปฏิเสธการให้บริการ การส่งสแปม การฉ้อโกงธุรกรรม และกิจกรรมอื่นที่คล้ายกันอาจเป็นอันตรายต่อธุรกิจได้ กิจกรรมเหล่านี้ใช้แบนด์วิธ ทำให้เซิร์ฟเวอร์ช้าลง และขโมยข้อมูลที่ละเอียดอ่อน ซึ่งนำไปสู่ความสูญเสียทางการเงินและความเสียหายต่อชื่อเสียงของบริษัท

# คำจำกัดความ

04

## ก่อนที่จะเจาะลึกเกี่ยวกับข้อมูล เรามากำหนดคำศัพท์สำคัญที่เราจะใช้อย่างแพร่หลายในรายงานนี้เป็นอันดับแรก

### บอทคืออะไร

ในบริบทของอินเทอร์เน็ต บอทคือแอปพลิเคชันซอฟต์แวร์ที่รันงานโดยอัตโนมัติ งานดังกล่าวมีตั้งแต่การดำเนินการง่าย ๆ เช่น การกรอกแบบฟอร์ม ไปจนถึงฟังก์ชันที่ซับซ้อนมากขึ้น เช่น การดึงข้อมูลจากเว็บไซต์

### Bad Bot คืออะไร

Bad Bot คือแอปพลิเคชันซอฟต์แวร์ที่ทำงานอัตโนมัติโดยมีเจตนาร้าย บอทเหล่านี้สามารถดึงข้อมูลจากเว็บไซต์โดยไม่ได้รับอนุญาตเพื่อนำมาใช้ซ้ำและทำให้มีข้อได้เปรียบทางการแข่งขัน มักใช้สำหรับการ Scalping ซึ่งเกี่ยวข้องกับการได้รับสินค้าที่มีจำนวนจำกัดและขายต่อในราคาที่สูงขึ้น Bad Bot ยังสามารถใช้เพื่อสร้างการโจมตีแบบปฏิเสธการให้บริการ (DDoS) แบบกระจายที่พุ่งเป้าไปที่แอปพลิเคชัน Bad Bot บางรายการทำกิจกรรมทางอาญา เช่น การฉ้อโกงและการโจรกรรมทันที ตัวอย่างหนึ่งก็คือบอทที่ดำเนินการกรอกข้อมูลประจำตัว ซึ่งเป็นหนึ่งในการโจมตีของบอทที่โดดเด่นที่สุด Open Web Application Security Project (OWASP) นำเสนอรายการการโจมตีของบอท 21 รายการที่ครอบคลุมในคู่มือภัยคุกคามอัตโนมัติ[1]

### Good Bot และ Bad Bot แตกต่างกันอย่างไร

ไม่ใช่บอททุกตัวที่พบในอินเทอร์เน็ตจะเป็นบอทที่แย่ ยังมีบอทดี ๆ ที่ให้บริการฟังก์ชันอันทรงคุณค่าอีกด้วย ตัวอย่างเช่น บอทบางรายการจัดทำดัชนีเว็บไซต์สำหรับเครื่องมือค้นหาหรือตรวจสอบประสิทธิภาพของเว็บไซต์ Googlebot และ Bingbot คือตัวอย่างโปรแกรมรวบรวมข้อมูลของเครื่องมือค้นหาที่ช่วยสร้างและรักษาดัชนีของหน้าเว็บที่สามารถค้นหาได้ ด้วยการจัดทำดัชนีหน้าเว็บ บอทเหล่านี้จะช่วยให้ผู้คนค้นหาชุดเว็บไซต์ที่เกี่ยวข้องมากที่สุดซึ่งตรงกับข้อความค้นหาของผู้สืบค้น บอทดังกล่าวมีความจำเป็นสำหรับธุรกิจออนไลน์ ช่วยให้ลูกค้าที่คาดหวังสามารถค้นหาและเข้าถึงเว็บไซต์ ผลิตภัณฑ์ และบริการของตนได้อย่างง่ายดาย

1 https://owasp.org/www-project-automated-threats-to-web-applications/

# แม้แต่ Good Bot ก็อาจทำให้เกิดความกังวลได้

Good Bot สามารถส่งผลกระทบอย่างมากต่อรายงานการวิเคราะห์เว็บ เนื่องจากสามารถทำให้บางเพจดูเป็นที่นิยมมากกว่าที่เป็นอยู่ได้ ตัวอย่างเช่น Good Bot อาจสร้างการแสดงผลสำหรับหน้าบนเว็บไซต์ของคุณที่คุณทำการโฆษณา แต่การคลิกโฆษณาดังกล่าวไม่เคยนำไปสู่ช่องทางการขาย เรื่องนี้อาจส่งผลให้ประสิทธิภาพลดลงในแง่ของผู้ลงโฆษณา และนำไปสู่การวิเคราะห์การตลาดที่ไม่ตรงตามความเป็นจริง ซึ่งท้ายที่สุดจะนำไปสู่การตัดสินใจที่ไม่ถูกต้อง ดังนั้นจึงจำเป็นอย่างยิ่งที่จะต้องแยกแยะระหว่างการเข้าเยี่ยมชมที่สร้างโดยผู้ใช้ที่เป็นมนุษย์ที่ถูกต้อง, Good Bot และ Bad Bot เพื่อประกอบการตัดสินใจทางธุรกิจโดยมีข้อมูลครบถ้วน

## การจำแนกประเภท Bad Bot

**Imperva สร้างระบบการจำแนกประเภทต่อไปนี้ซึ่งจัดหมวดหมู่ Bad Bot ตามระดับความซับซ้อน:**

### ธรรมดา

การเชื่อมต่อจากที่อยู่ IP ที่กำหนดโดย ISP เดียว บอทนี้จะเชื่อมต่อกับเว็บไซต์โดยใช้สคริปต์อัตโนมัติ บอทนี้จะไม่รายงานตนเองว่าเป็นเบราว์เซอร์

### ปานกลาง

บอทที่ซับซ้อนขึ้นไปจะใช้ซอฟต์แวร์ "เบราว์เซอร์เฮดเลส" ที่จำลองเทคโนโลยีเบราว์เซอร์ รวมถึงความสามารถในการรัน JavaScript

### ขั้นสูง

บอทที่ซับซ้อนที่สุดจะเลียนแบบพฤติกรรมผู้ใช้ของมนุษย์ เช่น การเคลื่อนไหวของเมาส์ และการคลิกเพื่อปลอมการตรวจจับบอท โดยใช้ซอฟต์แวร์อัตโนมัติของเบราว์เซอร์หรือมัลแวร์ที่ติดตั้งภายในเบราว์เซอร์จริงเพื่อเชื่อมต่อกับเว็บไซต์

### หลบเลี่ยง

*ผู้อยู่เบื้องหลังบอทที่มีความซับซ้อนมีความมุ่งมั่นและต่อเนื่องอย่างมาก หากโซลูชันการจัดการบอทบล็อกบอทในวันนี้ บอทอาจจะเข้าใจได้ว่าทำไมจึงถูกบล็อก และจะกลับมาในวันพรุ่งนี้พร้อมกับเทคนิคใหม่ในการหลบเลี่ยงการตรวจจับ ผู้กระทำการเหล่านี้ใช้ Bad Bot ขั้นสูง ซึ่งมีความยากในการตรวจจับมากขึ้นเนื่องจากความก้าวหน้าในเทคนิคการหลบหลีก พวกเขามักจะใช้เทคนิคต่างๆ ที่ใช้ร่วมกันระหว่าง Bad Bot ระดับปานกลางและขั้นสูง ดังนั้นเราจึงจัดกลุ่มบอทระดับปานกลางและขั้นสูงเพื่อให้ได้รับมุมมองใหม่เกี่ยวกับการวิเคราะห์ปริมาณการเข้าเยี่ยมชมของ Bad Bot*

*บอทหลบเลี่ยงใช้กลยุทธ์ที่ซับซ้อน เช่น ผ่านการหมุนเวียน IP แบบสุ่ม เข้าถึงผ่านทางพร็อกซีที่ไม่ระบุชื่อ ใช้พร็อกซีที่อยู่อาศัย เปลี่ยนแปลงข้อมูลระบุตัวตน เลียนแบบพฤติกรรมของมนุษย์ ชะลอคำขอ และไขปริศนา CAPTCHA ได้ พวกเขาใช้วิธีการ "ในระดับต่ำและช้า" เพื่อหลีกเลี่ยงการตรวจจับและดำเนินการโจมตีที่สำคัญโดยใช้คำขอน้อยลง วิธีนี้จะช่วยลด "การตรวจพบสัญญาณ" ที่เกิดจากการกระทำของ Bad Bot ทำให้ยากต่อการตรวจจับ*

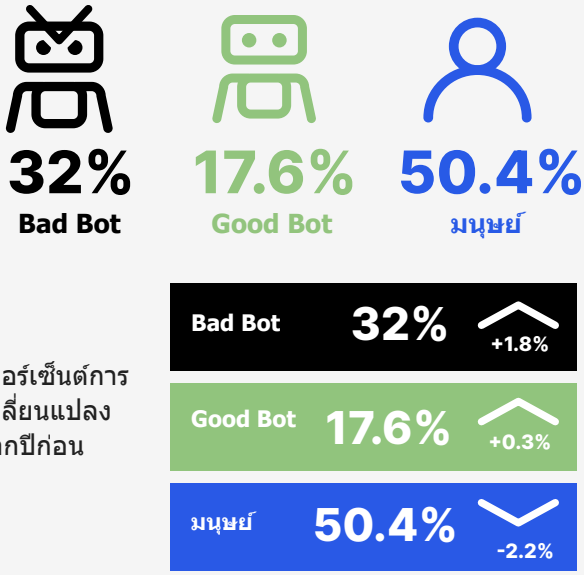
# ข้อมูลสรุปสำหรับผู้บริหาร

06

## ระดับการเข้าเยี่ยมชมของ Bad Bot ยังคงเพิ่มขึ้นอย่างต่อเนื่อง

ระดับการเข้าเยี่ยมชมของ Bad Bot เพิ่มขึ้นเป็นปีที่ 5 ติดต่อกัน ซึ่งบ่งบอกถึงแนวโน้มที่น่าตกใจ การเพิ่มขึ้นนี้ส่วนหนึ่งได้รับแรงผลักดันจากความนิยมที่เพิ่มขึ้นของปัญญาประดิษฐ์ (AI) และโมเดลการเรียนรู้ขนาดใหญ่ (LLM) ในปี 2023 Bad Bot มีสัดส่วน **32%** ของการเข้าเยี่ยมชมทางอินเทอร์เน็ตทั้งหมด – เพิ่มขึ้น **1.8%** จากปี 2022 สัดส่วนของปริมาณการใช้ Good Bot ก็เพิ่มขึ้นเช่นกัน แม้ว่าจะมีนัยสำคัญน้อยกว่าเล็กน้อยก็ตาม จาก **17.3%** ของปริมาณการเข้าชมโดยตั้งใจทั้งหมดในปี 2022 เป็น **17.6%** ในปี 2023 ทั้งคู่รวมกันเป็น **49.6%** ของการเข้าเยี่ยมชมทางอินเทอร์เน็ตทั้งหมดในปี 2023 ที่ไม่ใช่จากมนุษย์ เนื่องจากระดับการเข้าเยี่ยมชมของมนุษย์ลดลงเหลือ **50.4%** ของการเข้าเยี่ยมชมทั้งหมด

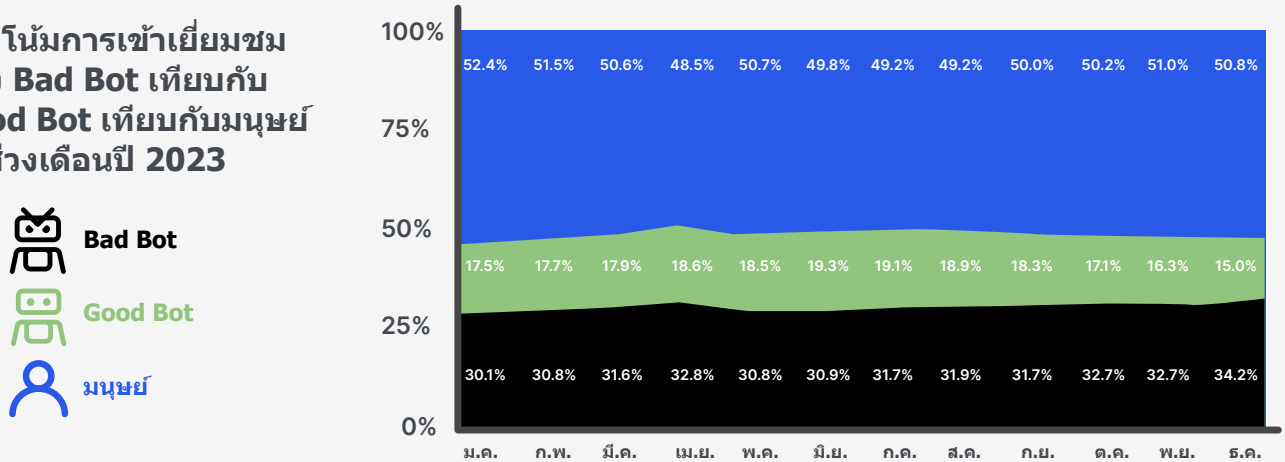
### การเข้าเยี่ยมชมของ Bad Bot เทียบกับ Good Bot เทียบกับมนุษย์ในปี 2023




## ระดับการเข้าเยี่ยมชมของ Bad Bot รายเดือน

แผนภูมิด้านล่างแสดงการวิเคราะห์แนวโน้มรายเดือนของโปรไฟล์ปริมาณการใช้อินเทอร์เน็ต สิ่งที่น่าสนใจก็คือการเข้าชมแบบอัตโนมัติมีมากกว่าการเข้าชมของมนุษย์ใน 4 เดือนที่แตกต่างกันตลอดทั้งปี ปริมาณการเข้าเยี่ยมชมของ Bad Bot ที่เพิ่มขึ้นในเดือนธันวาคม **(34.2%)** อาจเนื่องมาจากจำนวนการโจมตีที่เพิ่มขึ้นที่เราบันทึกได้ในเดือนนั้น และกิจกรรมของมนุษย์น้อยลงเล็กน้อยในช่วงเทศกาลวันหยุด

### แนวโน้มการเข้าเยี่ยมชมของ Bad Bot เทียบกับ Good Bot เทียบกับมนุษย์ในช่วงเดือนปี 2023

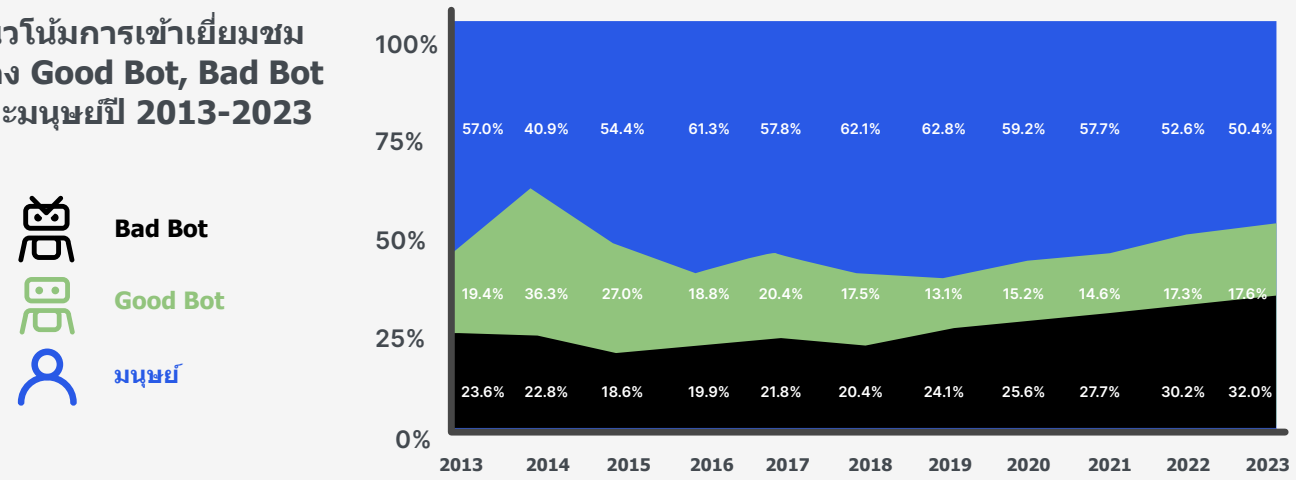


# การเข้าเยี่ยมชมของ Bad Bot ในช่วงหลายปีที่ผ่านมา

Imperva เป็นผู้นำในการต่อสู้กับ Bad Bot มานานกว่าทศวรรษ แผนภูมิด้านล่างแสดงแนวโน้มการเข้าเยี่ยมชมของ Good Bot, Bad Bot และมนุษย์ในช่วง 11 ปีที่ผ่านมา

ในปี 2013 ปริมาณการใช้อินเทอร์เน็ตประกอบด้วยการเข้าเยี่ยมชมของ Bad Bot **23.6%** Good Bot **19.4%** และมนุษย์ **57%** โดยเฉพาะอย่างยิ่งในปี 2014 ปริมาณการเข้าเยี่ยมชมของ Good Bot ได้เพิ่มขึ้นอย่างมาก โดยเพิ่มขึ้นจาก **20.98%** เป็น **36.32%** ซึ่งอาจได้รับอิทธิพลจากการจัดทำดัชนีเชิงรุกมากขึ้นโดยเครื่องมือค้นหา ปี 2015 การเข้าเยี่ยมชมของ Bad Bot ได้ลดลงจนถึงจุดต่ำสุดเมื่อมีการเข้าเยี่ยมชมของมนุษย์ถึง **54.4%** เนื่องจากมีผู้ใช้ใหม่เพิ่มขึ้น โดยเฉพาะจากจีน อินเดีย และอินโดนีเซีย ปี 2016 และ 2018 กิจกรรม Bad Bot ก็ลดลงเช่นกันที่ **19.9%** และ **20.4%** ตามลำดับ อย่างไรก็ตามตั้งแต่ปี 2019 ถึง 2023 ปริมาณการเข้าเยี่ยมชมของ Bad Bot เพิ่มขึ้นอย่างต่อเนื่อง โดยเพิ่มเป็น **32.0%** ของปริมาณการใช้อินเทอร์เน็ตทั้งหมดในปี 2023 ซึ่งสูงที่สุดเท่าที่เคยมีมา

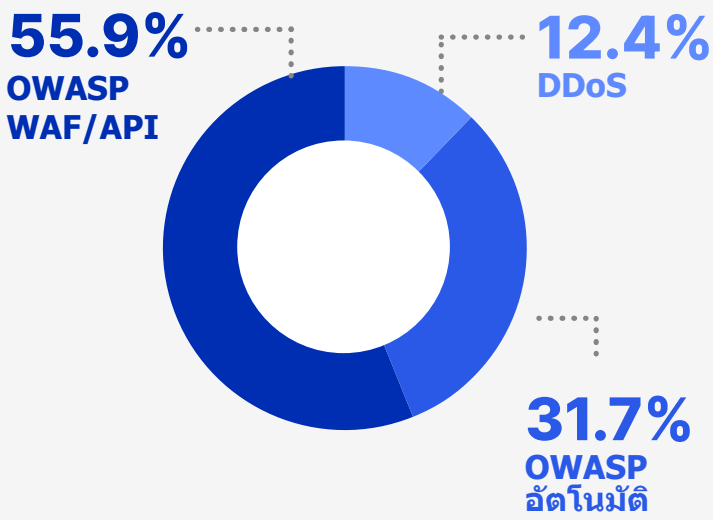
**แนวโน้มการเข้าเยี่ยมชมของ Good Bot, Bad Bot และมนุษย์ปี 2013-2023**




# ภัยคุกคามอัตโนมัติของ OWASP คิดเป็นเกือบหนึ่งในสามของการโจมตีทั้งหมด

จากการโจมตีทั้งหมดที่ Imperva บันทึกและบรรเทาได้ในปีที่ผ่านมา 31.7% เป็นภัยคุกคามอัตโนมัติ ตามที่ให้คำนิยามโดย OWASP การแยกแยะประเภทการโจมตีแสดงให้เห็นว่า **25%** ของการโจมตีที่บรรเทาลงคือ Bad Bot ที่ซับซ้อน ซึ่งพยายามใช้ตรรกะทางธุรกิจในทางที่ผิด

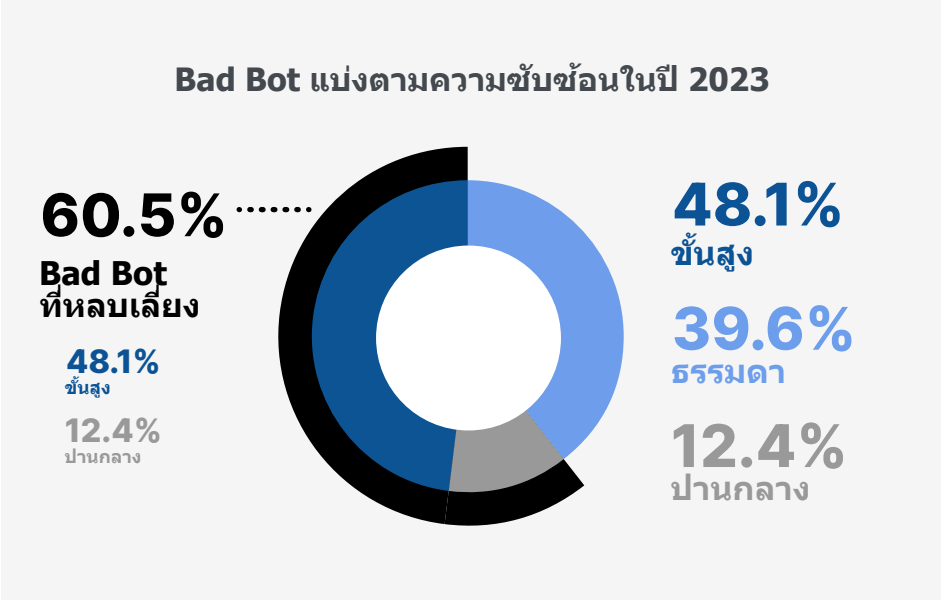
**การโจมตีลดลงในปี 2023 ตามหมวดหมู่**



# Bad Bot ที่มีความซับซ้อนปานกลางกำลังจะสูญพันธุ์หรือไม่

การนำเทคโนโลยี AI มาใช้เพิ่มมากขึ้นส่งผลต่อปริมาณ Bad Bot บนอินเทอร์เน็ตและระดับความซับซ้อนของบอทเหล่านั้น ทำให้เกิดการแบ่งแยกที่ชัดเจนระหว่างผู้กระทำการที่มีความซับซ้อนด้วยวิธีการและทรัพยากรในการปรับใช้บอทที่เป็นอันตรายขั้นสูงและผู้ที่ใช้เครื่องมือพื้นฐาน เช่น AI การสืบค้น เพื่อสร้างสคริปต์บอท ผลลัพธ์เป็นอย่างไร เราเห็นการเพิ่มขึ้นของ Bad Bot ธรรมดา ๆ ซึ่งมีสัดส่วน **39.6%** ของการเข้าเยี่ยมชมของ Bad Bot ในปี 2023 เทียบกับ **33.4%** ในปี 2022 เพิ่มขึ้น **26.3%** จาก 5 ปีก่อน แนวโน้มที่น่าสนใจข้อที่สองคือปริมาณของ Bad Bot ที่มีความซับซ้อนปานกลางได้ลดลง โดยลดลงจาก **15.3%** ในปี 2022 เป็น **12.4%** ในปี 2023 หากแนวโน้มนี้ดำเนินต่อไป เราอาจเห็นความชุกของบอทประเภทนี้ลดลงอย่างค่อยเป็นค่อยไป

บอทขั้นสูงได้ลดลงจาก **51.2%** ของการเข้าเยี่ยมชมของ Bad Bot ในปี 2022 เป็น **48.1%** ในปี 2023 การเปลี่ยนแปลงเหล่านี้ทำให้ Bad Bot มีสัดส่วน (ยอดรวมกันของระดับการเข้าเยี่ยมชมของบอทในระดับปานกลางและขั้นสูง) **60.5%** ของการเข้าเยี่ยมชมของ Bad Bot ทั้งหมด ซึ่งลดลงจากปีก่อน **(66.6%)** การเข้าเยี่ยมชมของ Bad Bot ยังคงมีความซับซ้อนสูง โดยมีความก้าวหน้าใหม่ ๆ เกิดขึ้นในแต่ละวันและเทคนิคการหลบเลี่ยงที่เกิดขึ้นใหม่ ๆ



# API เป็นเวกเตอร์ที่ชื่นชอบสำหรับการโจมตีบอท

ในปีที่ผ่านมา ภัยคุกคามอัตโนมัติเกิดขึ้น **30%** ของการโจมตี API จากข้อมูลดังกล่าว **17%** เป็น Bad Bot ที่ใช้ประโยชน์จากช่องโหว่ของตรรกะทางธุรกิจ ในขณะเดียวกัน **13%** เป็นภัยคุกคามอัตโนมัติประเภทอื่น ๆ การโจมตีเชิงตรรกะทางธุรกิจใช้ประโยชน์จากข้อบกพร่องภายในการออกแบบและการปรับใช้แอปพลิเคชัน ทำให้ผู้โจมตีสามารถจัดการฟังก์ชันการทำงานที่ถูกต้องตามกฎหมาย และอาจเข้าถึงข้อมูลที่ละเอียดอ่อนหรือบัญชีผู้ใช้ได้

การใช้ API เพื่อการสื่อสารที่ราบรื่นระหว่างแอปพลิเคชันและบริการต่าง ๆ เพิ่มขึ้น ทำให้โปรแกรมนี้เป็นองค์ประกอบสำคัญของการพัฒนาซอฟต์แวร์ เนื่องจาก API มีลักษณะตามธรรมชาติที่เครื่องสามารถอ่านได้ จึงเสี่ยงต่อการโจมตีจาก Bad Bot มากขึ้น การขาดการมองเห็นการเข้าเยี่ยมชม API ทำให้ตรวจจับได้ยาก อย่างไรก็ตาม การใช้ API อย่างแพร่หลายยังทำให้ตกเป็นเป้าหมายที่น่าสนใจสำหรับ Bad Bot อีกด้วย บอทที่เป็นอันตรายใช้ประโยชน์จาก API ซึ่งมักจะทำหน้าที่เป็นเส้นทางไปยังข้อมูลที่ละเอียดอ่อนโดยตรง ทำให้ API เสี่ยงต่อการใช้ตรรกะทางธุรกิจในทางที่ผิดและการฉ้อโกง API ทำให้มีพื้นที่การโจมตีเพิ่มขึ้น ทำให้มีจุดเริ่มต้นสำหรับการโจมตีอัตโนมัติมากขึ้น เนื่องจากองค์กรต่าง ๆ ยังคงพึ่งพา API อย่างมาก จึงจำเป็นอย่างยิ่งที่ต้องใช้มาตรการรักษาความปลอดภัยที่แข็งแกร่งเพื่อป้องกันภัยคุกคามที่ซับซ้อนเหล่านี้

# ปัญหา Bad Bot เป็นปัญหาในหลายอุตสาหกรรมและในหลายหน่วยงาน

Bad Bot ก่อให้เกิดภัยคุกคามร้ายแรงต่ออุตสาหกรรมต่าง ๆ และหน้าที่ขององค์กร โดยสามารถดำเนินกิจกรรมที่เป็นอันตรายด้วยความเร็วและขนาดที่เกินกว่าความสามารถของมนุษย์ ทำให้กลายเป็นเครื่องมือยอดนิยมสำหรับการละเมิดการใช้ในทางที่ผิด และการโจมตี

แม้ว่าบางกรณีการใช้งาน Bad Bot เช่น การคัดลอกเนื้อหาและการเข้าควบคุมบัญชีจะเป็นเรื่องปกติในอุตสาหกรรมต่าง ๆ แต่กรณีอื่น ๆ เช่น Scalping มักจะส่งผลกระทบต่ออุตสาหกรรมเฉพาะ เช่น การค้าปลีกและความบันเทิงออนไลน์ (การออกตั๋ว) อุตสาหกรรมบางประเภท เช่น สายการบิน มีกรณีการใช้งานเฉพาะ เช่น การโจมตีแบบ "การหมุนเวียนที่นั่ง" (โปรดดูที่ส่วน "ปริมาณการเข้าเยี่ยมชมของ Bad Bot ตามอุตสาหกรรม" สำหรับข้อมูลเพิ่มเติม)

### สัดส่วนที่ใหญ่ที่สุดของปริมาณการเข้าเยี่ยมชมของ Bad Bot ตามอุตสาหกรรมในปี 2023

| | |
|---|---|
| เกม | 57.2% |
| โทรคมนาคมและ ISP | 49.3% |
| คอมพิวเตอร์และไอที | 45.9% |
| ท่องเที่ยว | 44.5% |
| ชุมชนและสังคม | 42.2% |

### สัดส่วนที่ใหญ่ที่สุดของการเข้าเยี่ยมชมของ Bad Bot ขั้นสูงแยกตามอุตสาหกรรมในปี 2023

| | |
|---|---|
| กฎหมายและรัฐบาล | 75.8% |
| บันเทิง | 70.8% |
| บริการทางการเงิน | 67.1% |
| ท่องเที่ยว | 60.9% |
| การพนัน | 52.3% |

# พร็อกซีที่อยู่อาศัยเป็นเครื่องมือล่าสุดในคลังแสงของผู้อยู่เบื้องหลังบอทขั้นสูง

การเข้าเยี่ยมชมของ Bad Bot ที่มาจากพร็อกซีในที่พักอาศัยคิดเป็นสัดส่วนมากกว่าหนึ่งในสี่ของการเข้าเยี่ยมชมของ Bad Bot ทั้งหมด พร็อกซีที่อยู่อาศัยช่วยให้ผู้อยู่เบื้องหลังบอทหลบเลี่ยงการตรวจจับโดยทำให้ดูเหมือนว่าต้นทางของการเข้าเยี่ยมชมนั้นเป็นที่อยู่ IP ของที่อยู่อาศัยที่กำหนดโดย ISP อย่างถูกต้องตามกฎหมาย การทำเช่นนี้ทำให้เว็บไซต์และแพลตฟอร์มออนไลน์แยกความแตกต่างระหว่างการมีปฏิสัมพันธ์ของผู้ใช้จริงและพฤติกรรมบอทที่เป็นอันตรายได้ยากขึ้น

ความนิยมของเบราว์เซอร์มือถือในหมู่ผู้อยู่เบื้องหลัง Bad Bot ยังคงเพิ่มขึ้นอย่างต่อเนื่อง ในปี 2023 **44.8%** ของ Bad Bot พยายามหลบเลี่ยงการตรวจจับโดยปลอมตัวเป็นเบราว์เซอร์มือถือ ISP บนมือถือก็ยังคงได้รับความนิยมเช่นกัน โดยมีสัดส่วน **18.3%** ของการโจมตีที่เกิดขึ้น

| | |
|---|---|
| **Bad Bot ถูกรายงานว่าเป็นเอเยนต์ของผู้ใช้อุปกรณ์เคลื่อนที่** (Mobile Safari, Mobile Chrome ฯลฯ) | **44.8%** |
| **Bad Bot มาจาก ISP ที่อยู่อาศัย** | **25.8%** |
| **Bad Bot มาจาก ISP มือถือ** | **18.3%** |

## Bad Bot ทั่วโลก

สหรัฐถูกการโจมตีเพิ่มขึ้นในปีที่ผ่านมาหลังจากการโจมตีลดลงเป็นเวลาหลายปี โดยมีสัดส่วน **47%** ของการโจมตีด้วยบอททั้งหมดทั่วโลก เพิ่มขึ้นจาก **41.8%** ในปี 2022 เนเธอร์แลนด์เป็นประเทศใหม่ใน 5 อันดับแรกของปีนี้ โดยแซงหน้าออสเตรเลียไปอยู่ในอันดับที่ 2 ที่ **9%** ของการโจมตีของบอทโดยพุ่งเป้าไปที่ประเทศดังกล่าว ออสเตรเลียร่วงไปอยู่อันดับที่ 3 โดยตกเป็นเป้าหมายที่ **8.4%** ของการโจมตี ลดลงจาก **16.4%** ในปีก่อนและสอดคล้องมากขึ้นกับปีก่อนหน้า

### 5 อันดับแรก ตรงเป้าหมายมากที่สุด Bad Bot แยกตามประเทศ

| | |
|---|---|
| สหรัฐอเมริกา | 47% |
| เนเธอร์แลนด์ | 9% |
| ออสเตรเลีย | 8.4% |
| สหราชอาณาจักร | 5.1% |
| ฝรั่งเศส | 3.1% |

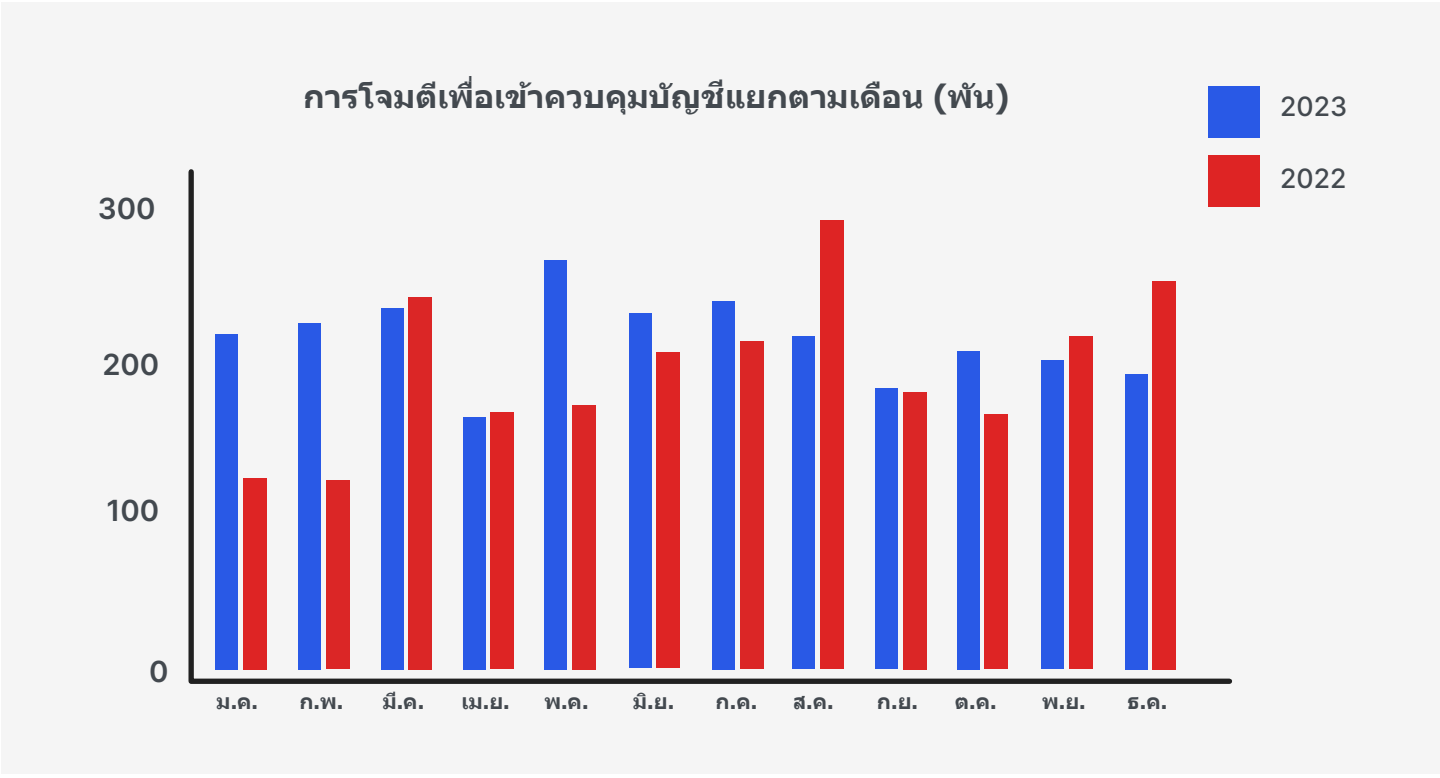
# การโจมตีเพื่อเข้าควบคุมบัญชี

# 11

การโจมตีเพื่อเข้าควบคุมบัญชี (ATO) เป็นหนึ่งในภัยคุกคามอัตโนมัติที่แพร่หลายที่สุด ซึ่งเกี่ยวข้องกับการใช้บอทเพื่อพยายามเข้าถึงและครอบครองบัญชีผู้ใช้โดยไม่ได้รับอนุญาตผ่านการกรอกข้อมูลประจำตัวและเทคนิคการถอดรหัสข้อมูลประจำตัว ส่งผลให้เกิดการขโมยข้อมูลประจำตัวดิจิทัลและการสูญเสียที่สำคัญสำหรับองค์กร การสูญเสียจากการโจรกรรมข้อมูลส่วนบุคคลคาดว่าจะสูงถึง 635.4 พันล้านดอลลาร์ในปี 2023 ตามข้อมูลของ Aite Group[2]

แผนภูมิต่อไปนี้แสดงถึงการโจมตีในรูปแบบ ATO รายเดือนที่ Imperva ทำการเก็บบันทึกในช่วงสองปีที่ผ่านมา การโจมตีเพิ่มขึ้น **10%** ระหว่างปี 2022 ถึง 2023 ถึงแม้ว่าจำนวนการโจมตีจะยังคงเพิ่มขึ้น แต่การเติบโตกลับมีนัยสำคัญน้อยกว่าในปีก่อนหน้า โดยถึงแม้จะเพิ่มขึ้นอย่างมากที่ **77%** และ **86%** ในเดือนมกราคมและกุมภาพันธ์ตามลำดับ เดือนพฤษภาคมและตุลาคมก็มีการโจมตีเพิ่มขึ้นเมื่อเทียบกับปี 2022 **(56% และ 25%)** ปีปฏิทิน 2023 จบลงด้วยการโจมตีที่ลดลง

เดือนสิงหาคม 2022 มีจำนวนการโจมตีสูงสุดในช่วง 2 ปีที่ผ่านมา การเพิ่มขึ้นนี้น่าจะเกิดจากการเพิ่มขึ้น **70%** ของการละเมิดข้อมูลทั่วโลกในช่วงเวลาดังกล่าว ดังที่ระบุไว้ในรายงานของปีที่ผ่านมา




2 https://aite-novarica.com/us-identity-theft-stark-reality#:~:text=Aite%20Group%20projects%20that%20losses%20from%20all%20identity,it%20from%20a%20simple%20fraudulent%20credit%20card%20transaction

# เกือบครึ่งหนึ่งของ ATO เป็นการโจมตีเป้าหมาย API โดยตรง

การโจมตีเพื่อเข้าควบคุมบัญชีที่พุ่งเป้าไปที่ API คิดเป็น 44% ของการโจมตีในรูปแบบ ATO ทั้งหมดที่บันทึกโดย Imperva เมื่อเทียบกับ **35%** ในปีก่อน การนำเอา API มาใช้อย่างแพร่หลายอันเนื่องมาจากการแพร่หลายของแอปพลิเคชันบนมือถือและเว็บ ทำให้ API กลายเป็นจุดเริ่มต้นที่น่าสนใจสำหรับผู้โจมตีที่ต้องการโจมตีบัญชีผู้ใช้ API เหล่านี้จัดการกระบวนการยืนยันตัวตนที่สำคัญ ซึ่งทำให้ตกเป็นเป้าหมายที่น่าสนใจ อย่างไรก็ตาม การใช้มาตรการรักษาความปลอดภัยถือเป็นเรื่องท้าทาย เนื่องจากความซับซ้อนของสภาพแวดล้อมไอทีสมัยใหม่ และลักษณะของแพลตฟอร์มออนไลน์ที่เชื่อมโยงถึงกัน เป็นผลให้อาชญากรไซเบอร์ใช้ประโยชน์จากช่องโหว่ใน API การพิสูจน์ตัวตนเพื่อเข้าถึงบัญชีผู้ใช้โดยไม่ได้รับอนุญาต พวกเขาใช้เทคนิคต่าง ๆ เช่น การยัดข้อมูลประจำตัว การโจมตีโดยการบังคับ หรือการใช้ API ในทางที่ผิด ความถี่ที่เพิ่มขึ้นของการโจมตีเพื่อเข้าควบคุมบัญชีโดยพุ่งเป้าไปที่ API การพิสูจน์ตัวตน เน้นย้ำถึงความจำเป็นสำหรับองค์กรในการปรับปรุงมาตรการรักษาความปลอดภัย API และปกป้องพวกเขาจากการโจมตีอัตโนมัติที่ซับซ้อนที่สุดในปัจจุบัน

### สถิติการโจมตีเพื่อเข้าควบคุมบัญชี

**10%** การเพิ่มขึ้นของการโจมตีเพื่อเข้าควบคุมบัญชีระหว่างปี 2022 ถึง 2023

**11%** เปอร์เซ็นต์ของความพยายามในการเข้าควบคุมบัญชีจากการเข้าสู่ระบบทั้งหมด

**44%** เปอร์เซ็นต์ของการโจมตีเพื่อเข้าควบคุมบัญชีที่พุ่งเป้าไปที่ API

### อุตสาหกรรมที่มีอัตราส่วน ATO สูงสุดจากการเข้าสู่ระบบทั้งหมด

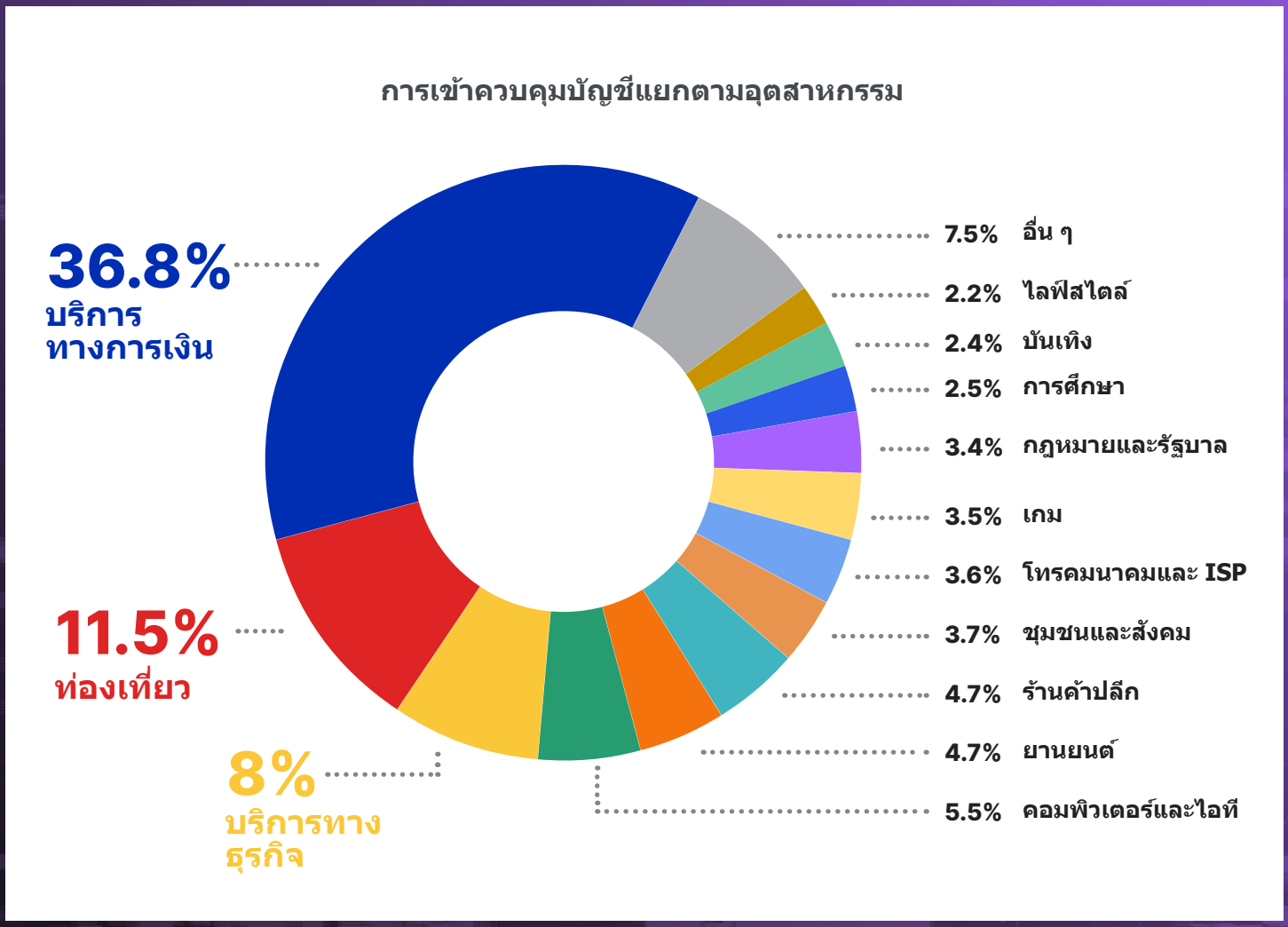
| | |
|---|---|
| บริการทางธุรกิจ | 38% |
| กีฬา | 35% |
| อาหารและร้านของชำ | 33% |
| คอมพิวเตอร์และไอที | 24% |
| การดูแลสุขภาพ | 18% |
| ท่องเที่ยว | 17% |

### ประเทศเป้าหมายส่วนใหญ่จากการโจมตีในรูปแบบ ATO

| | |
|---|---|
| สหรัฐอเมริกา | 40% |
| สหราชอาณาจักร | 7% |
| เยอรมนี | 7% |
| ออสเตรเลีย | 5% |
| สเปน | 5% |
| ประเทศไทย | 4% |

# อุตสาหกรรมที่ถูกโจมตีมากที่สุด

เมื่อเทียบกับอุตสาหกรรมที่มีอัตราส่วนการเข้าสู่ระบบที่เป็นอันตรายสูงสุดจากการเข้าสู่ระบบทั้งหมด แผนภูมิต่อไปนี้แสดงให้เห็นว่าอุตสาหกรรมใดประสบกับการโจมตีในรูปแบบ ATO ในปริมาณมากที่สุดในปี 2023 เมื่อพิจารณาจากแรงจูงใจเบื้องหลังบัญชีผู้ใช้ จึงไม่น่าแปลกใจที่บริการทางการเงินจะตกเป็นเป้าหมายมากที่สุด เช่นเดียวกับปีที่ผ่านมา โดยคิดเป็นสัดส่วน **36.8%** ของการโจมตีทั้งหมด อุตสาหกรรมการท่องเที่ยวเป็นอันดับสอง **(11.5%)** รองลงมาคือธุรกิจบริการ **(8%)** คอมพิวเตอร์และไอที **(5.5%)** ยานยนต์ **(4.7%)** และการค้าปลีก **(4.7%)**



# ความเสียหายจากการไม่ป้องกันการเข้าควบคุมบัญชี

หากคุณมีหน้าเข้าสู่ระบบ โอกาสที่หน้านั้นจะถูกโจมตีเพื่อเข้าควบคุมบัญชีนั้นจะมีสูง โอกาสจะยิ่งสูงขึ้นหากมีการแนบข้อมูลอันมีค่าหรือสิ่งจูงใจทางการเงินเข้ากับบัญชีผู้ใช้ของคุณ แต่ถึงกระนั้น หลายองค์กรก็หยุดชะงักในการป้องกันการโจมตีในรูปแบบ ATO ในเชิงรุก ซึ่งอาจทำให้ได้รับความเสียหายมหาศาล ตัวอย่างเช่น ลองพิจารณาสถานการณ์สมมติของการโจมตีในรูปแบบ ATO บนเว็บไซต์ที่ดำเนินธุรกิจในสหภาพยุโรป (EU) ความเสียหายที่อาจเกิดขึ้นอาจแตะระดับล้าน

ภายใต้กฎระเบียบ GDPR ค่าปรับสามารถสูงถึง **4%** ของมูลค่าการซื้อขายทั่วโลกประจำปีของบริษัทหรือ 20 ล้านยูโร แล้วแต่จำนวนใดจะมากกว่า สำหรับบริษัทที่มีมูลค่าการซื้อขายทั่วโลกต่อปีที่ 100 ล้านดอลลาร์ เฉพาะค่าปรับสูงสุดเพียงอย่างเดียวอาจอยู่ที่ 4 ล้านดอลลาร์

แต่ความเสียหายไม่ได้หยุดอยู่แค่เพียงเท่านั้น หากเหยื่อของการละเมิดยื่นฟ้องร้องดำเนินคดีแบบกลุ่ม ค่าเสียหายทั้งหมดที่เกิดขึ้นอาจสูงถึง 5 ล้านดอลลาร์ เมื่อพิจารณาจากค่าสินไหมทดแทนโดยเฉลี่ยที่ 500 ดอลลาร์ต่อลูกค้า 10,000 รายที่ได้รับผลกระทบ

ความเสียหายต่อชื่อเสียงเป็นอีกหนึ่งความเสียหายที่สำคัญซึ่งยากต่อการระบุจำนวน การสูญเสียความไว้วางใจจากลูกค้าอาจทำให้ยอดขายลดลงและมูลค่าหุ้นลดลง หากยอดขายลดลงที่ **10%** ในปีหน้าสำหรับบริษัทที่มีมูลค่าการซื้อขายทั่วโลกต่อปีที่ 100 ล้านดอลลาร์ อาจส่งผลให้ขาดทุนได้อีก 10 ล้านดอลลาร์ การลดลง **5%** ของมูลค่าหุ้นของบริษัทที่มีมูลค่าตลาด 200 ล้านดอลลาร์สหรัฐ เท่ากับการสูญเสีย 10 ล้านดอลลาร์สหรัฐ

สุดท้าย จะต้องพิจารณาค่าใช้จ่ายเพิ่มเติม เช่น ค่าใช้จ่ายในการแจ้งเตือน ค่าธรรมเนียมทางกฎหมายและที่ปรึกษา มาตรการรักษาความปลอดภัยที่เพิ่มขึ้น และบริการตรวจสอบเครดิตสำหรับลูกค้าที่ได้รับผลกระทบ สิ่งเหล่านี้อาจรวมกันได้อีก 2.5 ล้านดอลลาร์สหรัฐ

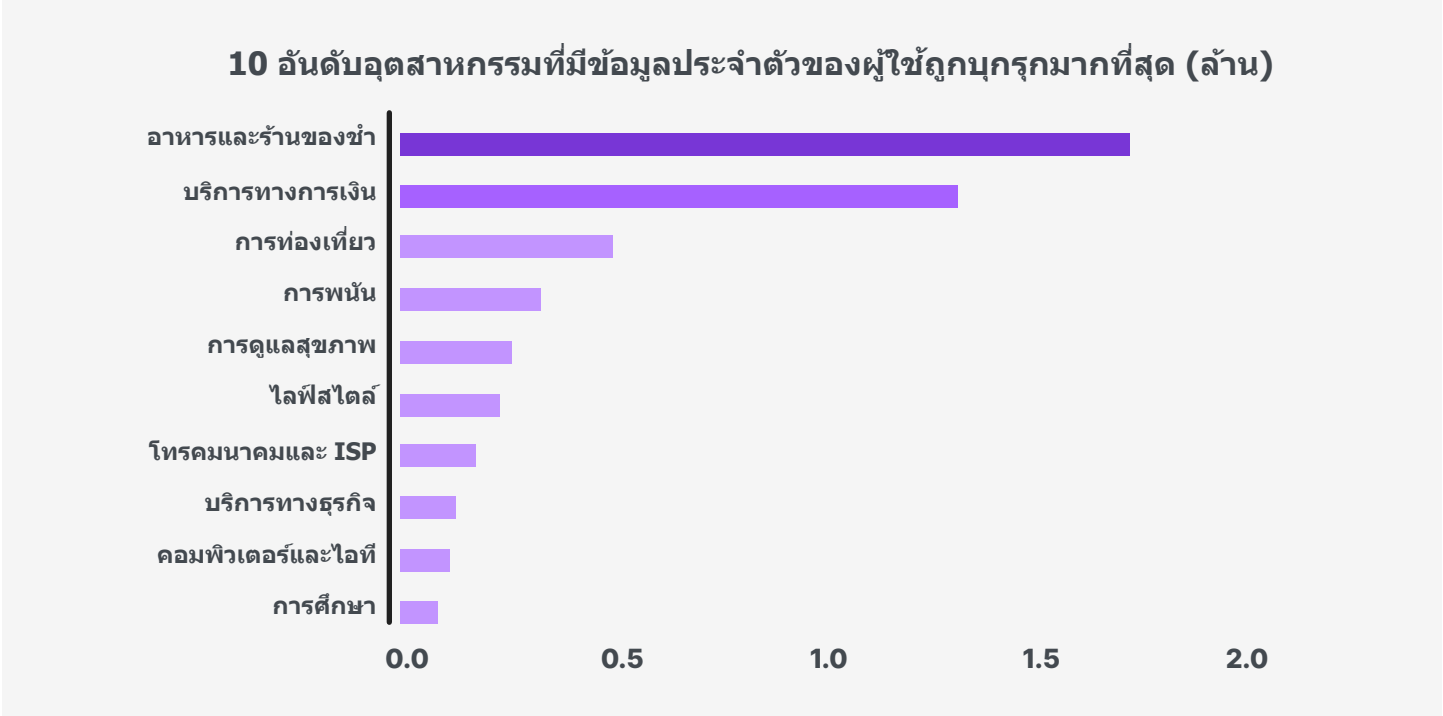
# Passkeys จะส่งผลต่อการโจมตีเพื่อเข้าควบคุมบัญชีที่กำลังแพร่หลายได้อย่างไร

การนำเอา Passkeys[3,4] มาใช้มีวัตถุประสงค์เพื่อปรับปรุงประสบการณ์ผู้ใช้ออนไลน์และลดความเสี่ยงของการฉ้อโกงในการเข้าควบคุมบัญชี Passkeys เป็นตัวเลือกที่สะดวกและปลอดภัยกว่าในส่วนของการใช้รหัสผ่าน โดยทำงานบนแพลตฟอร์มและเบราว์เซอร์หลักทั้งหมด ทำให้ผู้ใช้สามารถเข้าสู่ระบบโดยการปลดล็อคคอมพิวเตอร์หรืออุปกรณ์มือถือด้วยลายนิ้วมือ การจดจำใบหน้า หรือรหัส PIN ในเครื่อง ซึ่งจะช่วยแบ่งเบาภาระของผู้ใช้ที่เกิดจากรหัสผ่านแบบเดิม โดยช่วยลดความยากลำบากในการเลือกและการเรียกคืนรหัสผ่านที่คาดเดายากสำหรับหลายบัญชี

ด้วยการรวมรหัสผ่านเข้ากับกระบวนการพิสูจน์ตัวตน องค์กรต่าง ๆ จะสามารถลดความเสี่ยงของบัญชีจากการพยายามเข้ายึดครองได้ รวมทั้งเพิ่มความแข็งแกร่งให้กับมาตรการรักษาความปลอดภัย และปกป้องข้อมูลผู้ใช้ อย่างไรก็ตาม การนำ Passkeys ไปใช้อย่างกว้างขวางในแพลตฟอร์มและบริการออนไลน์ต่าง ๆ เป็นสิ่งจำเป็นสำหรับการเพิ่มประสิทธิภาพ องค์กรต่าง ๆ ต้องการความพยายามร่วมกันในการปรับใช้และรวมระบบ Passkeys เข้ากับกระบวนการพิสูจน์ตัวตนของตน เนื่องจากองค์กรต่าง ๆ หันมาใช้เทคโนโลยีนี้มากขึ้น จึงเป็นเรื่องน่าสนใจที่จะเห็นผลกระทบจากการโจมตีเพื่อเข้าควบคุมบัญชีอย่างแพร่หลาย ทั้งนี้ เริ่มมีสัญญาณเริ่มแรกของการชะลอตัวของการเติบโตเกี่ยวกับจำนวนการโจมตี แม้ว่าจะยังเร็วเกินไปที่จะเป็นบทสรุปขั้นสุดท้ายก็ตาม หนึ่งสิ่งที่ชัดเจน: ด้วยสถานะความปลอดภัยในปัจจุบัน การเข้าควบคุมบัญชียังคงเป็นภัยคุกคามที่สำคัญต่อองค์กรและผู้ใช้ปลายทาง การเฝ้าระวังและมาตรการเชิงรุกมีความสำคัญอย่างยิ่งในการป้องกันการโจมตีที่อาจเกิดขึ้น

# บัญชีผู้ใช้ที่ถูกบุกรุก

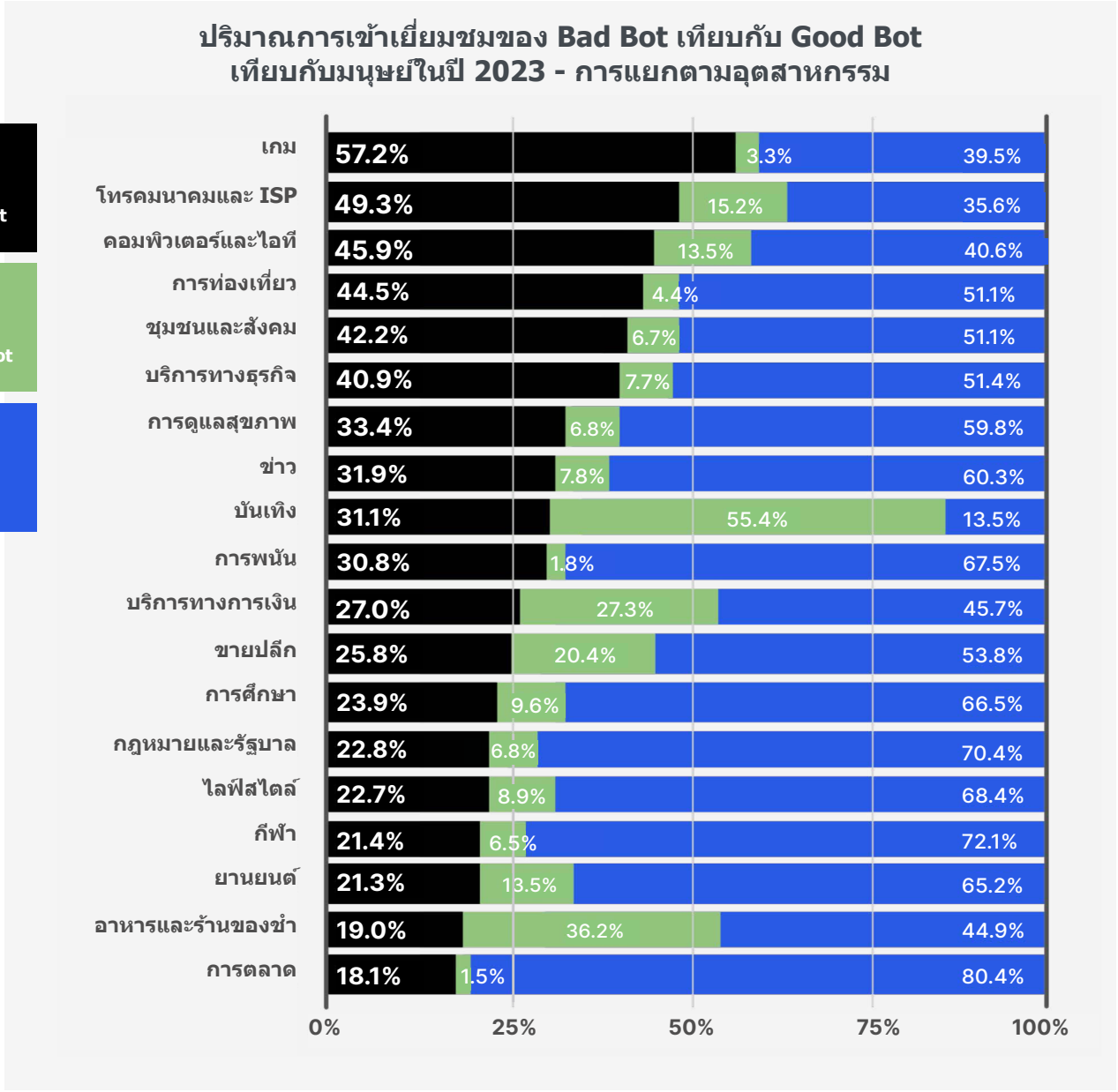
การตรวจจับบัญชีผู้ใช้ที่ถูกบุกรุกจากการละเมิดข้อมูลออนไลน์สามารถช่วยให้องค์กรต่างๆ ปรับปรุงมาตรการรักษาความปลอดภัยและป้องกันการโจมตีเพื่อเข้าควบคุมบัญชีที่กำลังจะเกิดขึ้นได้ แผนภูมิด้านล่างแสดง 10 อันดับอุตสาหกรรมแรกที่มีบัญชีที่ถูกบุกรุกมากที่สุดซึ่งได้รับการระบุและแจ้งเตือนโดย Imperva




3 https://fidoalliance.org/passkeys/
4 https://developers.google.com/identity/passkeys

# ปริมาณการเข้าเยี่ยมชมของ Bad Bot แยกตามอุตสาหกรรม

แต่ละอุตสาหกรรมมีปัญหา Bad Bot แตกต่างกัน แผนภูมิต่อไปนี้แสดงโปรไฟล์การเข้าเยี่ยมชมที่ Imperva เก็บบันทึกระหว่างปี 2023 ในมุมมองแยกย่อยตามอุตสาหกรรม โดยให้ภาพรวมอย่างใกล้ชิดว่าระดับการเข้าเยี่ยมชมของ Bad Bot โดยรวมที่เพิ่มขึ้นโดยรวมส่งผลกระทบต่อแต่ละอุตสาหกรรมอย่างไร



**เว็บไซต์เกม**และวิดีโอเกมกลับมาอยู่ในอันดับต้น ๆ อีกครั้งในรายงาน Bad Bot ประจำปีนี้ คล้ายกับปีที่ผ่านมา **(58.7%)** การเข้าเยี่ยมชมเว็บไซต์เกมมีสัดส่วนที่สูง **(57.2%)** ที่เกิดจาก Bad Bot บอทสามารถสร้างปัญหาโดยการเข้ายึดบัญชีผู้ใช้ สร้างบัญชีปลอมเพื่อใช้ประโยชน์จากสิทธิประโยชน์และการโกง บอทสามารถทำในสิ่งที่ยากหรือเป็นไปไม่ได้สำหรับผู้เล่นที่เป็นมนุษย์ เช่น มีปฏิสัมพันธ์กับเกมด้วยความเร็วสูงเพื่อเอาชนะผู้เล่นที่เป็นมนุษย์ หรือทำฟาร์มสกุลเงิน ไอเทม หรือคะแนนประสบการณ์ (XP) เสมือนอย่างต่อเนื่อง การกระทำเหล่านี้ทำให้ผู้เล่นที่เป็นมนุษย์ไม่เพลิดเพลินอย่างแท้จริง ซึ่งท้ายที่สุดก็จะจากไป ส่งผลให้จำนวนผู้เล่นและการมีส่วนร่วมลดลง ซึ่งส่งผลให้สูญเสียรายได้

อุตสาหกรรม**คอมพิวเตอร์และไอที** พบว่าปริมาณการเข้าเยี่ยมชมของ Bad Bot เพิ่มขึ้นในปี 2023 ซึ่งคิดเป็น**45.9%** ของปริมาณการเข้าชมทั้งหมดซึ่งสูงกว่าระดับของปีที่ผ่านมาที่ **40%** Bad Bot เป็นอันตรายต่ออุตสาหกรรม นำไปสู่ปัญหาทางเทคนิค การฉ้อโกง และความเสี่ยงด้านความปลอดภัย วิธีหนึ่งที่พบบ่อยที่สุดที่ Bad Bot พุ่งเป้าไปที่อุตสาหกรรมก็คือผ่านการโจมตีแบบปฏิเสธการให้บริการ (DDoS) แบบกระจาย โดยที่บอทจำนวนมากจะส่งคำขอจนท่วมเซิร์ฟเวอร์ของเว็บไซต์ นอกจากนี้ Bad Bot ยังดูดข้อมูลที่ละเอียดอ่อน เช่น ข้อมูลการเข้าสู่ระบบและข้อมูลส่วนบุคคล ซึ่งอาจนำไปสู่การละเมิดข้อมูลและการขโมยข้อมูลประจำตัวที่อาจเกิดขึ้นได้ นอกจากนี้ ผู้ไม่ประสงค์ดียังใช้บอทเพื่อสแกนช่องโหว่และการฉ้อโกงการคลิก ส่งผลให้การวัดผลบิดเบือนและเกิดการสูญเสียรายได้

อุตสาหกรรม**โทรคมนาคมและ ISP** ประสบกับปริมาณการเข้าเยี่ยมชมเพิ่มขึ้นเล็กน้อยจาก Bad Bot ในปี 2022 เปอร์เซ็นต์ของการเข้าเยี่ยมชมของ Bad Bot อยู่ที่ **47.7%** และเพิ่มขึ้นเป็น **49.3%** ในปี 2023 อุตสาหกรรมนี้ประกอบด้วย ISP มือถือ, ISP ที่พักอาศัย, ผู้ให้บริการโฮสติ้ง และอื่น ๆ Bad Bot พุ่งเป้าไปที่อุตสาหกรรมนี้ด้วยกิจกรรมที่เป็นอันตรายต่าง ๆ ซึ่งรวมถึงการคัดลอกข้อมูลลูกค้าที่ละเอียดอ่อนและการโจมตีเข้าสู่ระบบโดยการบังคับเพื่อเข้ายึดบัญชีผู้ใช้ เนื่องจากอุตสาหกรรมนี้ต้องพึ่งพาความพร้อมใช้งานสูงและมีความอ่อนไหวต่อการหยุดทำงาน Bad Bot จึงสามารถเริ่มต้นการโจมตีแบบ Distributed Denial-of-Service (DDoS) เพื่อครอบงำโครงสร้างพื้นฐานและขัดขวางบริการต่าง ๆ บอทมักจะปลอมตัวเป็นผู้ใช้ที่ถูกต้อง ทำให้แยกแยะระหว่างการเข้าเยี่ยมชมของแท้และปลอมได้ยาก นอกจากนี้ การเข้าเยี่ยมชมของบอทยังสามารถบิดเบือนการวิเคราะห์เว็บไซต์ ซึ่งนำไปสู่การตัดสินใจที่ผิดพลาด

อุตสาหกรรม**การท่องเที่ยว**ฟื้นตัวเต็มที่จากปีที่ท้าทายเป็นเวลาหลายปี ผู้คนเดินทางมากขึ้นกว่าเดิม[5,6] น่าเสียดายที่เรื่องนี้ได้รับความสนใจจากบอทมากขึ้นด้วย เนื่องจากเว็บไซต์ท่องเที่ยวพบว่าปริมาณการเข้าเยี่ยมชมของ Bad Bot เพิ่มขึ้นอย่างมากในปีนี้ จาก **37.4%** ของการเข้าเยี่ยมชมเว็บทั้งหมดไปอยู่ที่ **44.5%** อุตสาหกรรมการท่องเที่ยวมักจะต้องต่อสู้กับปัญหาบอทที่ซับซ้อนอยู่เสมอ เนื่องจากผู้ไม่ประสงค์ดีสามารถใช้ประโยชน์จากตรรกะทางธุรกิจต่าง ๆ ในแอปพลิเคชันการเดินทางได้

ในส่วนของอุตสาหกรรมการท่องเที่ยว **สายการบิน**มักจะตกเป็นเป้าหมายเป็นพิเศษ ปัญหาหลักมาจากแพลตฟอร์มออนไลน์ของสายการบิน ซึ่งรวมถึงเว็บไซต์ แอปมือถือ และ API แพลตฟอร์มเหล่านี้เป็นที่ที่ลูกค้าเข้าถึงข้อมูลเที่ยวบิน ตัดสินใจซื้อ และจองเที่ยวบิน น่าเสียดายที่บอทมักจะพุ่งเป้าไปที่แพลตฟอร์มเหล่านี้เพื่อดูดข้อมูล รบกวนบริการ และบางครั้งก็ทำการฉ้อโกงด้วย

ปัญหาสำคัญที่สายการบินต้องเผชิญคือบอทดูดข้อมูลจำนวนมากที่เข้าถึงคุณสมบัติเว็บของตนโดยไม่ได้รับอนุญาต บอทเหล่านี้มาจากแหล่งต่าง ๆ เช่น Online Travel Agencies (OTA) ผู้รวบรวมข้อมูล และคู่แข่ง บอทดูดข้อมูลเที่ยวบินในปริมาณมากทำให้เกิดปัญหามากมาย รวมถึงสร้างความเสียหายให้กับข้อมูลเชิงลึกทางธุรกิจ เช่น อัตราส่วนการดูต่อการจอง และค่าธรรมเนียมที่เพิ่มขึ้นสำหรับผู้ให้บริการการจองของบุคคลที่สาม ในปีที่ผ่านมา เราได้แชร์เรื่องราวของสายการบินแห่งหนึ่งซึ่งมี API การค้นหาที่ถูกบอทเก็บรวบรวมข้อมูลเที่ยวบินอย่างหนัก ส่งผลให้มีการเรียกเก็บค่าบริการรายเดือนสำหรับคำขอ API จากผู้จัดหาที่เป็นบุคคลที่สามมากกว่า 500,000 ดอลลาร์ เราเห็นการโจมตีที่คล้ายกันซึ่งมุ่งเป้าไปที่สายการบินอื่นในปีนี้

การเปลี่ยนแปลงอย่างกะทันหันของอัตราส่วนการดูต่อการจองสามารถบ่งชี้ได้ว่าปริมาณการเข้าเยี่ยมชมของบอทกำลังดึงข้อมูลเที่ยวบินอย่างแข็งขัน นี่เป็นปัญหาสำคัญสำหรับหลายสายการบิน ในขณะที่ OTA และผู้รวบรวมข้อมูลที่ได้รับอนุญาตสามารถดึงข้อมูลภายใต้เงื่อนไขที่ตกลงกันไว้ แต่ผู้ที่ไม่ได้รับอนุญาตจะใช้บอทเพื่อดึงข้อมูลราคาและข้อมูลเที่ยวบินโดยไม่มีข้อตกลง กิจกรรมที่ไม่ได้รับอนุญาตนี้ฝ่าฝืนข้อกำหนดของสายการบินและบิดเบือนตัวชี้วัดทางธุรกิจและข้อมูลเชิงลึกที่สำคัญ สายการบินคู่แข่งยังอาจใช้บอทเพื่อรวบรวมข้อมูลการตลาดแบบเรียลไทม์ได้อีกด้วย บอทจะดูดข้อมูลราคาของคู่แข่ง ที่นั่งคงเหลือ และค่าโดยสารลดราคา ส่งผลให้ปริมาณการเข้าเยี่ยมชมของบอทเพิ่มขึ้น และไม่ตอบสนองวัตถุประสงค์อันมีค่าแก่สายการบินที่ตกเป็นเหยื่อ

**กิจกรรมบอทที่สร้างความเสียหายมากที่สุดมาจากอาชญากรที่ปล่อยตัวบอทเพื่อทำให้เกิดช่องโหว่กับโปรแกรมสะสมคะแนนแลกรับรางวัล**

กิจกรรมบอทที่สร้างความเสียหายมากที่สุดมาจากอาชญากรที่ปล่อยตัวบอทเพื่อทำให้เกิดช่องโหว่กับโปรแกรมสะสมคะแนนแลกรับรางวัล บอทเหล่านี้ใช้การยัดข้อมูลประจำตัวโดยการบังคับและโจมตีหน้าเข้าสู่ระบบเพื่อเข้าถึงบัญชี ขโมยคะแนนสะสม และกระทำการซื้อสินค้าที่เป็นการฉ้อโกง

กรณีการใช้ Bad Bot อย่างหนึ่งในอุตสาหกรรมการบินก็คือการหมุนเวียนที่นั่ง ปัญหานี้แพร่หลายอย่างยิ่งโดยเฉพาะในภูมิภาคเอเชียแปซิฟิก บอทการหมุนเวียนที่นั่งจะเข้ายึดที่นั่งโดยไม่ชำระเงิน ซึ่งมักจะใช้เวลานานถึง 24 ชั่วโมง บอทเหล่านี้ช่วยให้ผู้กระทำการ เช่น OTA ที่ไม่ได้รับอนุญาต สามารถระงับและขายต่อการจองได้โดยไม่ต้องลงทุน ผลกระทบจะเห็นได้ชัดเจนที่สุดก็คือเมื่อถึงเวลาออกเดินทาง เที่ยวบินที่ดูเหมือนจะจองเต็มกลับมีที่นั่งว่างมากขึ้นเรื่อย ๆ การหมุนเวียนที่นั่งทำให้สูญเสียรายได้และสร้างความเสียหายต่อชื่อเสียงของสายการบิน

ในภาพรวม ผลกระทบของบอทต่ออุตสาหกรรมการบินนั้นกว้างมาก โดยนำไปสู่การดูดข้อมูลโดยไม่ได้รับอนุญาต การหมุนเวียนที่นั่ง การเข้าควบคุมบัญชี และการฉ้อโกง กิจกรรมเหล่านี้ขัดขวางประสบการณ์ของลูกค้าและทำให้ชื่อเสียงของสายการบินเสื่อมเสีย ปัญหานี้สามารถนำไปสู่ประสิทธิภาพของเว็บไซต์และแม้กระทั่งการหยุดทำงานหากปล่อยทิ้งไว้โดยไม่ดำเนินการ

5 https://www.washingtonpost.com/climate-environment/2023/11/23/pandemic-flying-normal-emissions/
6 https://www.euronews.com/travel/2023/04/21/post-covid-revenge-travel-has-gone-big-and-the-revenge-is-sweet

**เว็บไซต์ชุมชนและสังคม** มีสัดส่วน **42.2%** ของการเข้าเยี่ยมชมจาก Bad Bot เพิ่มขึ้นเล็กน้อยจาก**41.4%** ในปีที่ผ่านมา Bad Bot ประเภทหนึ่งที่พบบ่อยที่สุดคือสแปมบอทหรือที่เรียกว่าสแปมข่าวปลอมและสแปมความคิดเห็น บอทเหล่านี้แพร่กระจายข่าวปลอม ขยายการโฆษณาชวนเชื่อ และปกปิดเนื้อหาที่เป็นอันตราย เช่น มัลแวร์ภายในลิงก์คลิกเบท ปัญหานี้พบแพร่หลายแม้กระทั่งในองค์กรไม่แสวงหาผลกำไรที่เปิดรับการบริจาคบนเว็บไซต์ของพวกเขา บอทใช้ประโยชน์จากหน้าการบริจาคเพื่อทดสอบหมายเลขบัตรเครดิตที่ถูกขโมย ซึ่งทำให้องค์กรที่ไม่หวังผลกำไรมีภาระทางการเงินจำนวนมาก

อุตสาหกรรม**การดูแลสุขภาพ**เห็นการเพิ่มขึ้นของปริมาณการเข้าเยี่ยมชมของ Bad Bot ด้วยเช่นกัน โดยมี **33.4%** ของการเข้าชมเว็บไซต์ที่มาจาก Bad Bot เมื่อเปรียบเทียบกับ**31.7%** ในปีที่ผ่านมา Bad Bot ซึ่งพุ่งเป้าไปที่อุตสาหกรรมการดูแลสุขภาพมักจะมุ่งหวังที่จะได้รับข้อมูลที่ละเอียดอ่อนของลูกค้า ซึ่งอาจส่งผลให้เกิดการละเมิดข้อมูลได้ บอทเหล่านี้สามารถควบคุมบัญชีผู้ใช้เพื่อเข้าถึงบันทึกทางการแพทย์หรือดึงข้อมูลสุขภาพที่เป็นความลับ เช่น บันทึกผู้ป่วย ประวัติการรักษาพยาบาล และรายละเอียดการประกันภัย ข้อมูลที่ถูกขโมยนี้สามารถนำไปขายบนเว็บมืดเพื่อหากำไรหรือนำไปใช้ในกิจกรรมฉ้อโกงได้ นอกจากนี้ Bad Bot ในการดูแลสุขภาพยังเป็นภัยคุกคามจากการโอเวอร์โหลดระบบผ่านการโจมตีแบบ Distributed Denialof-Service (DDoS) ซึ่งทำให้ผู้ป่วยและผู้ให้บริการด้านการดูแลสุขภาพเข้าถึงข้อมูลและบริการที่สำคัญได้ยาก

อุตสาหกรรม**บริการทางการเงิน**มีสัดส่วนของ Bad Bot ที่ **27%** ของการเข้าชมเว็บไซต์ในปี 2023 สิ่งที่น่าสนใจก็คือปริมาณการเข้าเยี่ยมชมเกือบเท่ากันนั้นมาจาก Good Bot ซึ่งอาจเป็นผลมาจากผู้รวบรวมข้อมูลทางการเงินและผู้ให้บริการอื่น ๆ ที่ใช้บอทเพื่อให้ข้อมูลอันมีค่าและข้อมูลเชิงลึกแก่ผู้ใช้ แต่เมื่อพูดถึง Bad Bot อุตสาหกรรมนี้ต้องเผชิญกับภัยคุกคามที่สำคัญจากการโจมตีเพื่อเข้าควบคุมบัญชี Bad Bot ใช้เทคนิคการเข้าสู่ระบบโดยการบังคับ เช่น การยัดข้อมูลประจำตัวหรือการถอดรหัสข้อมูลประจำตัวเพื่อพยายามเข้าถึงบัญชีผู้ใช้อย่างผิดกฎหมาย ภัยคุกคามทั่วไปอื่น ๆ รวมไปถึง การฉ้อโกงบัตรเครดิตและการขโมยเนื้อหาที่กำหนดเอง เช่น การเปลี่ยนแปลงอัตราดอกเบี้ยบ่อยครั้ง ภัยคุกคามอัตโนมัติอีกประการหนึ่งที่พุ่งเป้าไปที่อุตสาหกรรมคือบอทการเก็งกำไรที่พุ่งเป้าไปที่การแลกเปลี่ยนสกุลเงินดิจิทัลและตลาด NFT บอทเหล่านี้ใช้การดูดข้อมูลจากเว็บเพื่อระบุความไม่สมดุลของราคาระหว่างการแลกเปลี่ยนและตลาดที่แตกต่างกัน ช่วยให้ผู้ประกอบการสามารถทำกำไรจากการซื้อขาย crypto และ NFT จากการแลกเปลี่ยนในตลาดหนึ่งไปยังอีกตลาด โดยใช้ประโยชน์จากความแตกต่างด้านราคาระหว่างเหรียญเดียวกันหรือคู่ในการแลกเปลี่ยนที่ต่างกันเพื่อทำกำไร

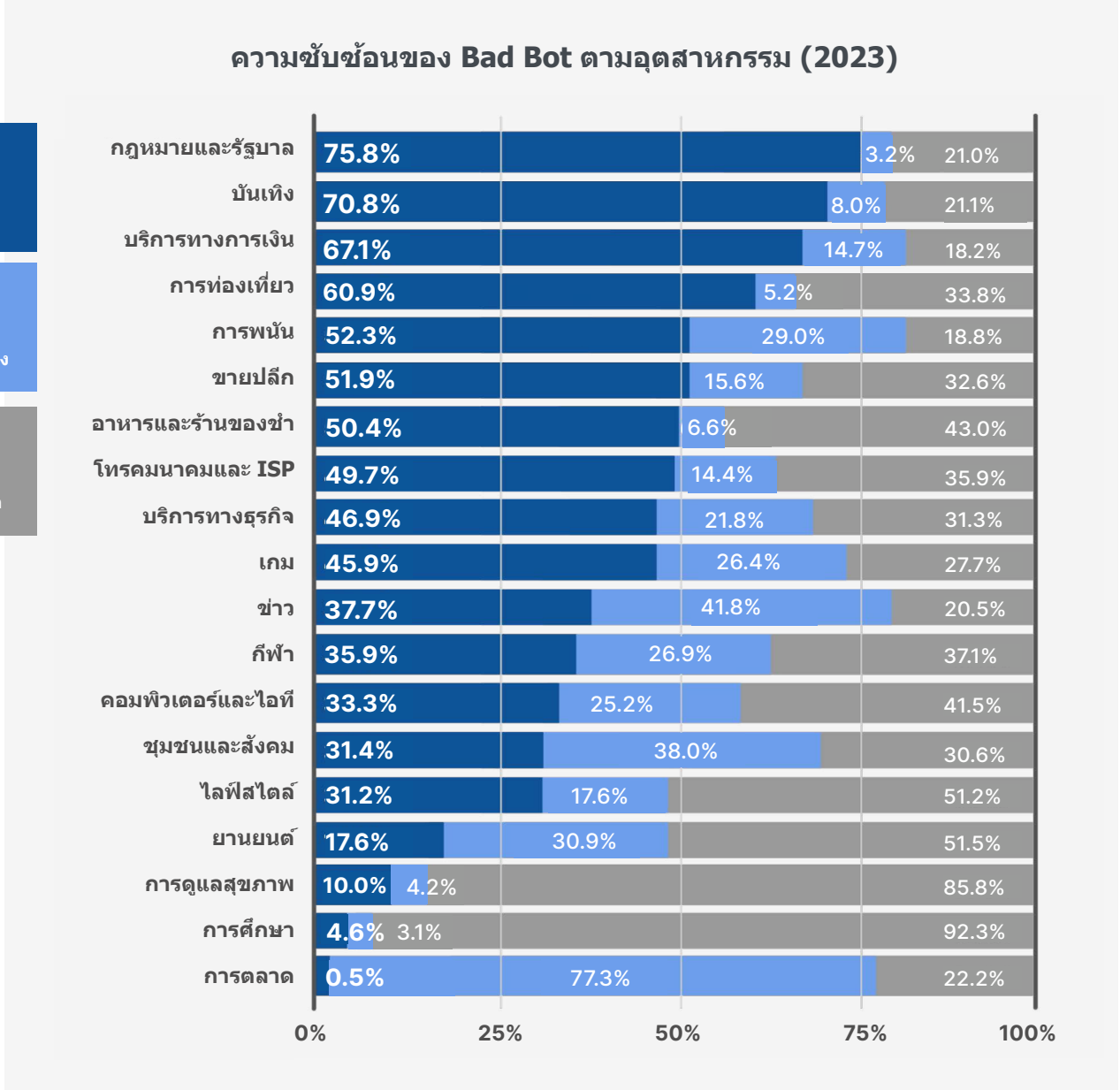
อุตสาหกรรม**ขายปลีก**มีสัดส่วนกว่าหนึ่งในสี่ **(25.8%)** ของการเข้าชมเว็บไซต์มาจาก Bad Bot ซึ่งเพิ่มขึ้นจาก **22.7%** ในปีที่ผ่านมา เช่นเดียวกับปีที่ผ่านมา ผู้ค้าปลีกออนไลน์ก็ประสบปัญหาปริมาณการเข้าเยี่ยมชมของ Good Bot เช่นกัน **(20.4%)** สาเหตุน่าจะมาจากความแพร่หลายของโปรแกรมรวบรวมข้อมูลเปรียบเทียบราคาที่เครื่องมือค้นหาและเว็บไซต์ใช้ ผู้ค้าปลีกออนไลน์ต้องเผชิญกับภัยคุกคามอัตโนมัติในรูปแบบต่าง ๆ ที่ส่งผลเสียต่อธุรกิจของตน และเป็นอุปสรรคต่อประสบการณ์และการดำเนินการของลูกค้า Bad Bot ถูกใช้สำหรับกิจกรรมที่เป็นอันตรายต่าง ๆ เช่น การคัดลอกข้อมูลโดยคู่แข่ง การได้รับสินค้าที่มีจำนวนจำกัดเพื่อขายต่อในราคาที่สูงกว่า (Scalping) การโจมตีโดยการปฏิเสธการให้บริการแบบกระจาย (DDoS) และมีส่วนร่วมในกิจกรรมทางอาญา เช่น การถอดรหัสบัตรเครดิต การทำบัตร การถอดรหัสบัตรของขวัญ และการเข้าควบคุมบัญชี (ATO) การโจมตีเพื่อเข้าควบคุมบัญชี (ATO) เพิ่มขึ้นในช่วงเทศกาลวันหยุดปีนี้ การโจมตีในรูปแบบ ATO เพิ่มขึ้นตั้งแต่เดือนกันยายน โดยมีกิจกรรมการโจมตีพุ่งสูงขึ้นอย่างมีนัยสำคัญที่บันทึกได้ในวันที่ 8, 14 และ 24 พฤศจิกายน (Black Friday) จำนวนการโจมตีในวัน Black Friday เป็นเรื่องที่น่าประหลาดใจที่ **85%** เพิ่มขึ้นเมื่อเทียบกับ **66%** ของการโจมตีในรูปแบบ ATO ที่เพิ่มขึ้นในช่วง Black Friday ของปี 2022 นอกจากนี้ ความรุนแรงของการโจมตีเหล่านี้ยังเพิ่มขึ้นอีกด้วย โดยจำนวนคำขอเข้าสู่ระบบที่เป็นอันตรายเพิ่มสูงขึ้น **82%** ในช่วงระหว่างเดือนตุลาคมถึงพฤศจิกายน

อุตสาหกรรม**บันเทิง**ประกอบด้วยแพลตฟอร์มการจำหน่ายตั๋ว บริการสตรีมมิ่ง บริษัทผู้ผลิต และสถานที่จัดงาน เช่นเดียวกับปีที่ผ่านมา อุตสาหกรรมมีปริมาณการใช้ระบบอัตโนมัติในปริมาณที่สูงมาก ซึ่งทั้ง Good Bot **(55.4%)** และ Bad Bot **(31.1%)** คิดเป็น**86.5%** ของการเข้าเยี่ยมชมทั้งหมด เพิ่มขึ้นจาก **83.4%** สาเหตุที่มี Good Bot ในปริมาณมากอาจเกี่ยวข้องกับการที่บุคคลที่สามต่าง ๆ ทำการคัดลอกเว็บไซต์บันเทิงเพื่อเปรียบเทียบราคา ข้อมูลการวางจำหน่ายสินค้า และการให้คำแนะนำแก่ผู้บริโภค เว็บไซต์ที่ตกเป็นเป้าหมายมากที่สุดในอุตสาหกรรมนี้คือเว็บไซต์จำหน่ายตั๋ว อุตสาหกรรมบันเทิงเป็นหนึ่งในอุตสาหกรรมแรก ๆ ที่ตกเป็นเป้าหมายของ Bad Bot บอท Scalping ตัวตรวจสอบรายการที่นั่ง และบอทกรอกข้อมูลประจำตัวที่เข้าถึงบัญชีผู้ใช้เป็นบอทที่แพร่หลายมากที่สุดในเว็บไซต์เหล่านี้

# ความซับซ้อนของ Bad Bot แยกตามอุตสาหกรรม

แผนภูมิต่อไปนี้แสดงรายละเอียดการเข้าเยี่ยมชมของ Bad Bot ตามระดับความซับซ้อน ยิ่งสัดส่วนของ Bad Bot ขั้นสูงสูงขึ้นเท่าไร ปัญหาบอทก็จะยิ่งซับซ้อนมากขึ้นสำหรับอุตสาหกรรม การวิเคราะห์ที่ครอบคลุมนี้ให้ความกระจ่างมากขึ้นเกี่ยวกับความเสี่ยงจาก Bad Bot ที่อุตสาหกรรมต่าง ๆ เผชิญในปีนี้

สิ่งสำคัญก็คือต้องเข้าใจว่าไม่จำเป็นต้องมีความสัมพันธ์กันระหว่างความซับซ้อนของการเข้าเยี่ยมชมของ Bad Bot กับปริมาณการเข้าเยี่ยมชมในตัวของมันเอง หรือกล่าวอีกนัยหนึ่งก็คือ อุตสาหกรรมที่มีปริมาณการเข้าเยี่ยมชมของ Bad Bot จำนวนมากอาจถูกจัดประเภทว่าเป็นบอทธรรมดาทั้งหมด อย่างไรก็ตาม สิ่งสำคัญก็คือต้องไม่ลืมว่าการเข้าเยี่ยมชมของบอทขั้นสูงก่อให้เกิดความเสี่ยงที่สำคัญ ไม่ว่าปริมาณการใช้งานจะน้อยเพียงใด ซึ่งเป็นเพราะว่า Bad Bot ขั้นสูงสามารถบรรลุเป้าหมายได้ด้วยคำขอที่น้อยกว่า Bad Bot ทั่วๆ ไป และมีความเพียรพยายามในการบรรลุเป้าหมายตามที่กำหนดไว้มากกว่ามาก

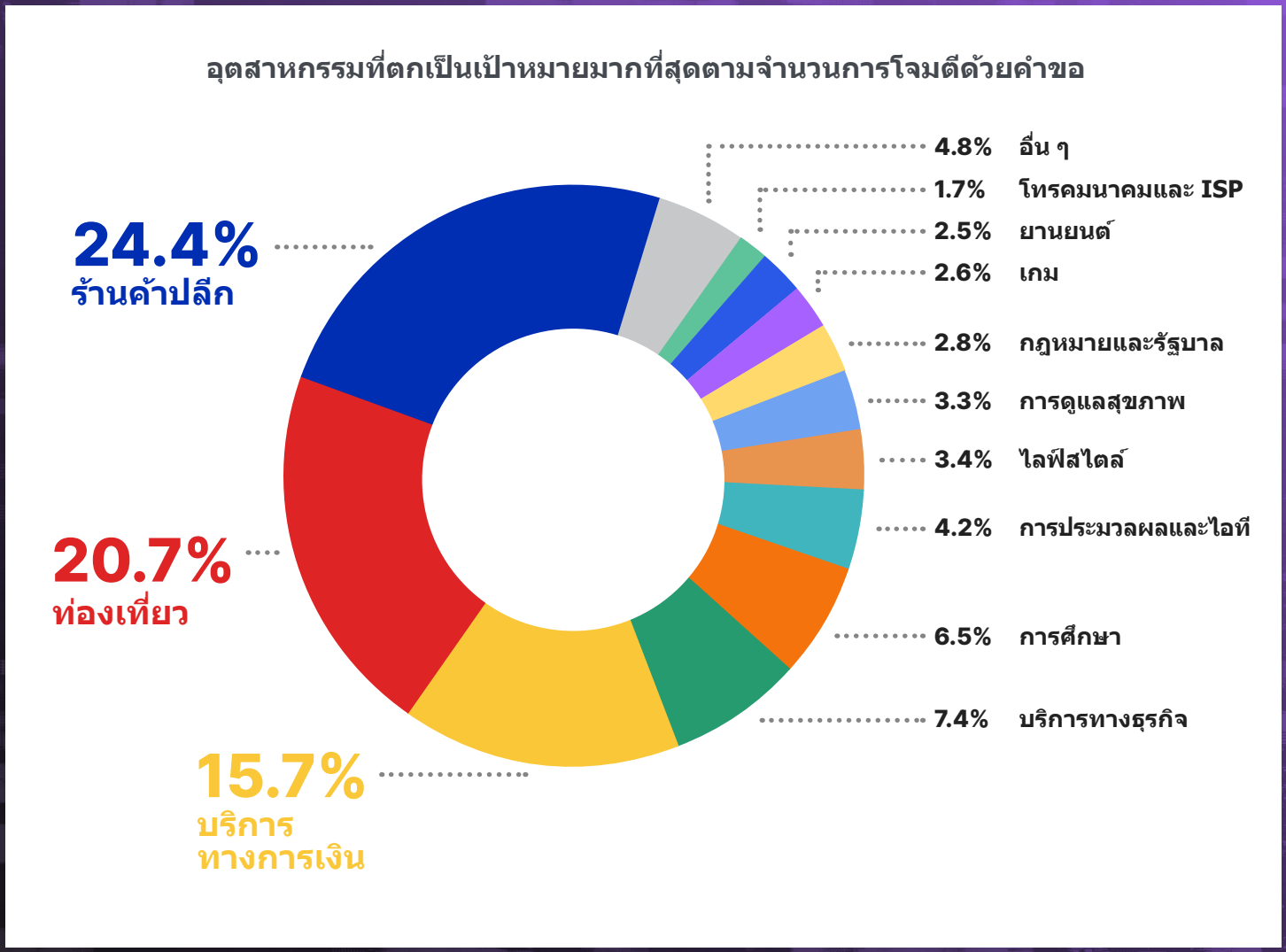


# อุตสาหกรรมที่ตกเป็นเป้าหมายการโจมตีของบอทมากที่สุด

รายละเอียดโปรไฟล์การเข้าเยี่ยมชมสำหรับแต่ละอุตสาหกรรมจะแสดงอัตราส่วนของการเข้าเยี่ยมชมของบอทต่อการเข้าเยี่ยมชมทั้งหมด ในทางตรงกันข้าม การกระจายการโจมตีด้วยบอทในอุตสาหกรรมต่าง ๆ จะให้มุมมองที่แตกต่างออกไป บ่งชี้ว่าอุตสาหกรรมใดตกเป็นเป้าของการโจมตีของบอทที่ใหญ่ที่สุด เช่นเดียวกับปีที่ผ่านมา การค้าปลีก การท่องเที่ยว และบริการทางการเงินเป็นอุตสาหกรรมที่เป็นเป้าหมายมากที่สุดสามอันดับแรก

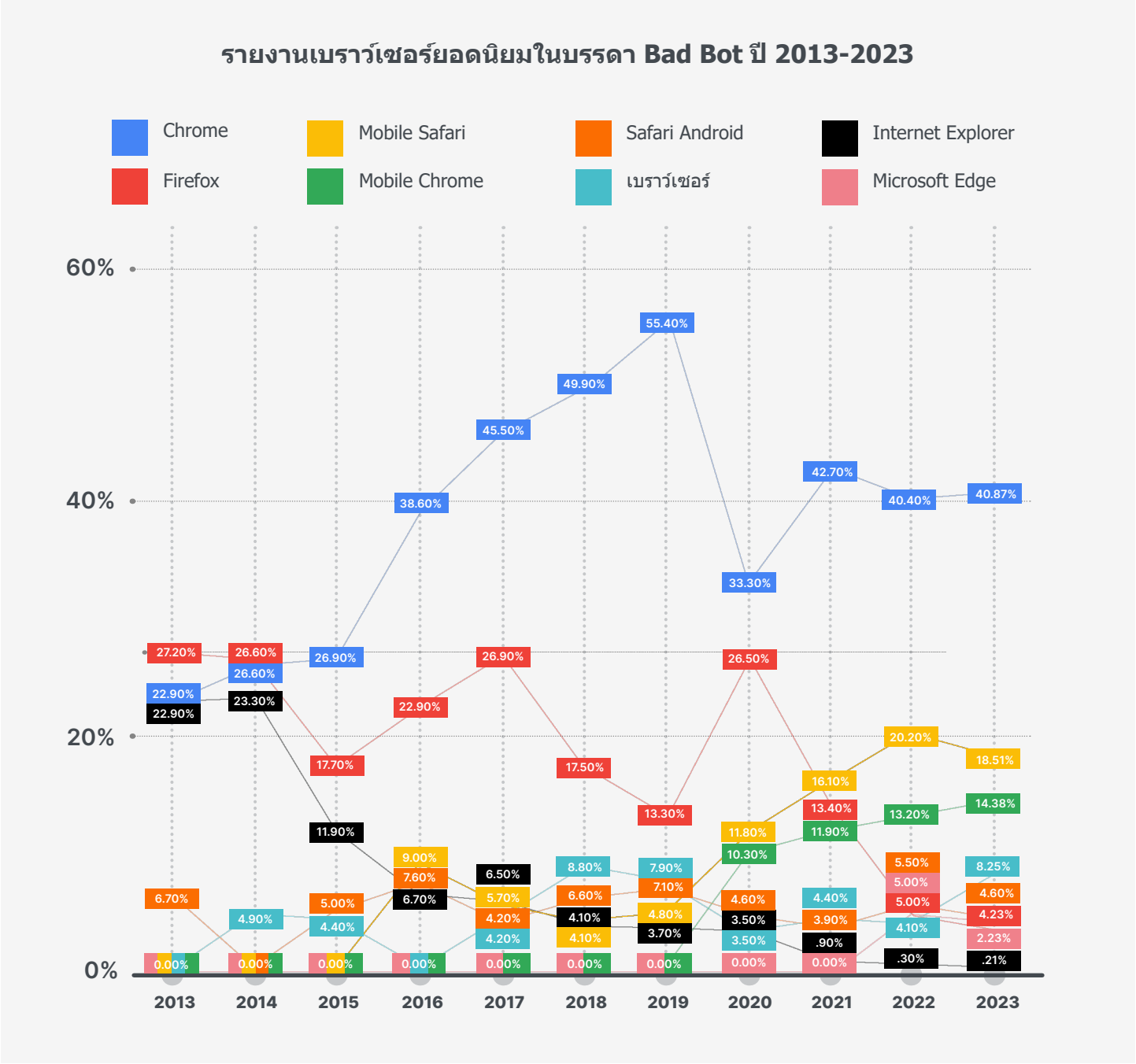
ตามรายละเอียดในส่วนก่อนหน้านี้ อุตสาหกรรมเหล่านี้เผชิญกับปัญหาบอทที่ซับซ้อน โดยมีกรณีการใช้บอทหลายกรณีที่คุกคามผลกำไร ทั้ง 3 อุตสาหกรรมมีอันดับสูงในด้านความซับซ้อนของบอทบนเว็บไซต์ของพวกเขา

สิ่งสำคัญก็คือต้องทราบว่าอุตสาหกรรมที่มีอัตราส่วน Bad Bot สูง ไม่จำเป็นต้องสอดคล้องกับการตกเป็นเป้าหมายมากหรือน้อยกว่าอุตสาหกรรมอื่น ๆ อุตสาหกรรมอาจมีอัตราส่วนการเข้าเยี่ยมชมของบอทต่ำ เนื่องจากมีการเข้าเยี่ยมชมจากคนจำนวนมากตลอดทั้งปี หรืออาจถูกกำหนดเป้าหมายโดย Bad Bot ขั้นสูงกว่าซึ่งใช้คำขอน้อยกว่าก็สามารถได้ผลลัพธ์ที่ต้องการ



# เบราว์เซอร์ Chrome และ Android บนมือถือได้รับความนิยมเพิ่มขึ้น

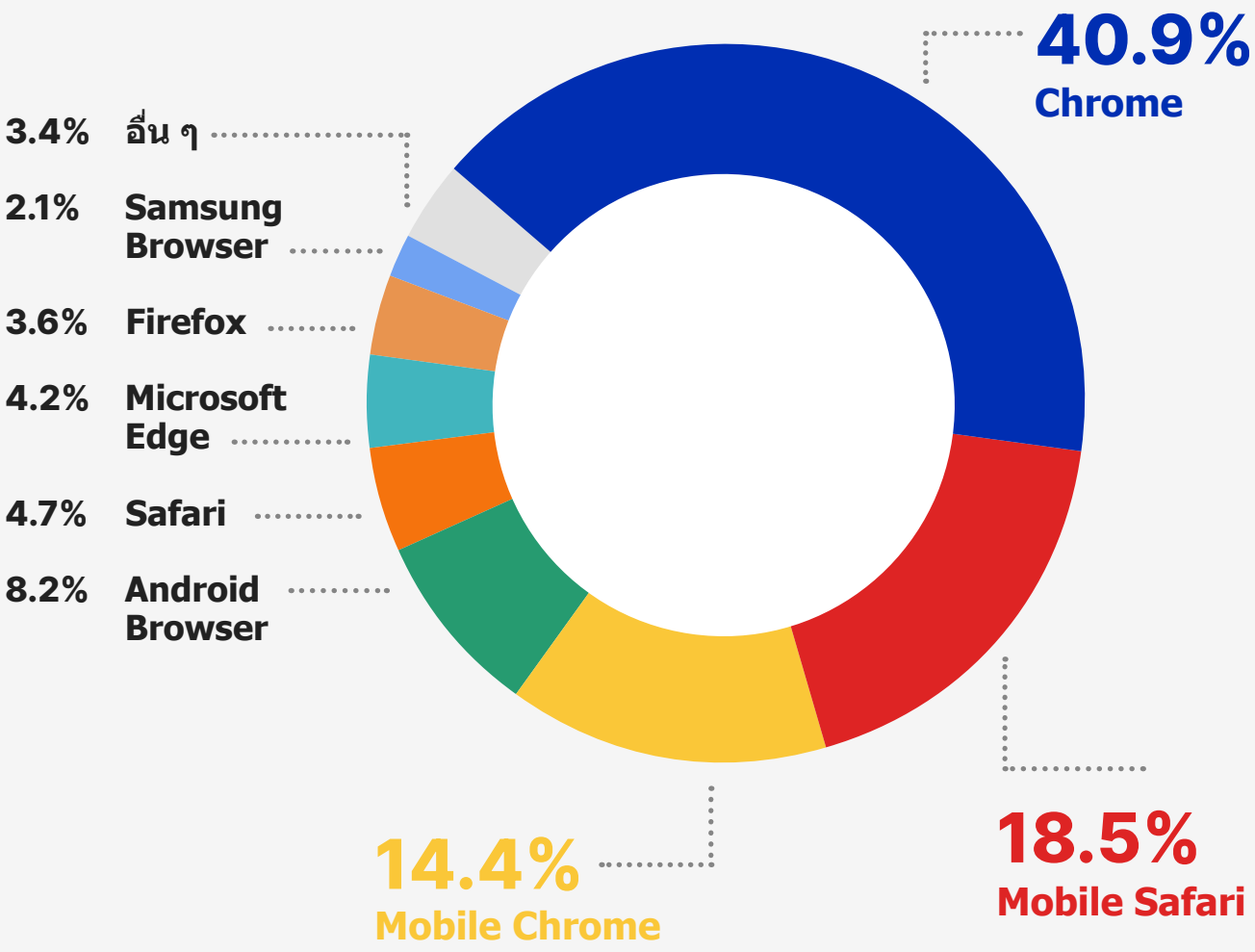
Bad Bot ใช้เทคนิคต่าง ๆ เพื่อหลบเลี่ยงการตรวจจับ หนึ่งในนั้นคือการปลอมตัวเป็นผู้ใช้ที่ถูกต้องตามกฎหมายโดยรายงานตัวเองไปยังต้นทางว่าเป็นเว็บหรือเบราว์เซอร์มือถือที่มนุษย์ใช้กันทั่วไป บอทบรรลุเป้าหมายนี้โดยใช้ซอฟต์แวร์อัตโนมัติของเบราว์เซอร์ เทคนิคนี้กลายเป็นเรื่องปกติในบรรดา Bad Bot ส่วนมาก แม้ว่าครั้งหนึ่งจะเคยเป็นวิธีการหลบหลีกขั้นสูงก็ตาม สิ่งที่น่าสนใจก็คือแนวโน้มความนิยมของเบราว์เซอร์ในบรรดา Bad Bot ได้เปลี่ยนแปลงไปในช่วงทศวรรษที่ผ่านมา ซึ่งสะท้อนให้เห็นถึงการเปลี่ยนแปลงในการตั้งค่าของผู้ใช้และแนวโน้มอื่น ๆ ที่ช่วยให้บอทหลบเลี่ยงการตรวจจับ ตัวอย่างเช่น Internet Explorer ครั้งหนึ่งเคยเป็นเบราว์เซอร์ยอดนิยมในหมู่มนุษย์และ Bad Bot แต่เรื่องนี้ไม่เป็นความจริงอีกต่อไป



ในช่วงสองปีที่ผ่านมา เราได้เห็นความนิยมเพิ่มขึ้นของเว็บเบราว์เซอร์บนมือถือท่าม กลาง Bad Bot เริ่มต้นด้วยความนิยมที่เพิ่มขึ้นของ Bad Bot ที่เลือกใช้ Mobile Safari **(18.51%)** เป็นเบราว์เซอร์ที่เลือก และได้ขยายอย่างรวดเร็วไปยัง Mobile Chrome (14.38%) **และ** Android Browser (8.25%)

การใช้งาน Chrome โดย Bad Bot ยังคงอยู่ที่ระดับเดิมที่ **40.87%** ของการเข้าเยี่ยมชมของ Bad Bot ทั้งหมด ในขณะที่ Firefox ยังคงลดความนิยมลง **(3.57%)**

**อุตสาหกรรมที่ตกเป็นเป้าหมายมากที่สุดตามจำนวนการโจมตีด้วยคำขอ**



# เอเยนต์ของผู้ใช้อุปกรณ์เคลื่อนที่คิดเป็นเกือบครึ่งหนึ่งของปริมาณการเข้าเยี่ยมชมของบอท

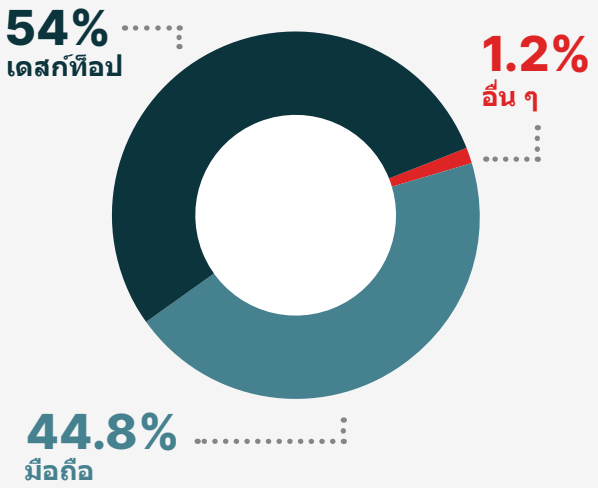
Bad Bot ปลอมตัวเป็นตัวแทนผู้ใช้มือถือ **44.8%** ของการเข้าเยี่ยมชมของ Bad Bot ทั้งหมด ความแพร่หลายของบอทเพิ่มขึ้นอย่างมากจาก **28.1%** ในปี 2020 เป็น **44.8%** ในปี 2023 ความนิยมที่เพิ่มขึ้นมี 2 เหตุผลที่สำคัญ ข้อแรก Bad Bot พยายามเลียนแบบลักษณะการเข้าเยี่ยมชมของมนุษย์อย่างใกล้ชิด ณ เดือนกุมภาพันธ์ 2024 กว่า **55%** ของการเข้าเยี่ยมชมอินเทอร์เน็ตมาจากอุปกรณ์เคลื่อนที่[7] พวกเราส่วนใหญ่ใช้โทรศัพท์มือถือของเราในการท่องอินเทอร์เน็ต ดังนั้นจึงเป็นเรื่องสมเหตุสมผลที่บอทจะทำเช่นเดียวกันเพื่อผสมผสานกับการเข้าชมของมนุษย์ การแยกระหว่างเอเยนต์มือถือและเดสก์ท็อปนั้นใกล้เคียงกันมากเมื่อพิจารณาจากปริมาณการเข้าเยี่ยมชมของ Bad Bot

เหตุผลที่สองเกี่ยวข้องกับความเป็นส่วนตัว เว็บเบราว์เซอร์บางรายการ เช่น Mobile Safari มีการควบคุมความเป็นส่วนตัวและฟีเจอร์เพิ่มเติมที่ทำให้ Bad Bot สามารถซ่อนตัวตนที่แท้จริงได้ง่ายขึ้น เนื่องจากเบราว์เซอร์เหล่านี้อาจส่งแอตทริบิวต์ไปยังที่มาของเว็บไซต์น้อยลง ซึ่งทำให้การสร้างลายนิ้วมือที่แม่นยำของอุปกรณ์มีความท้าทายมากขึ้น

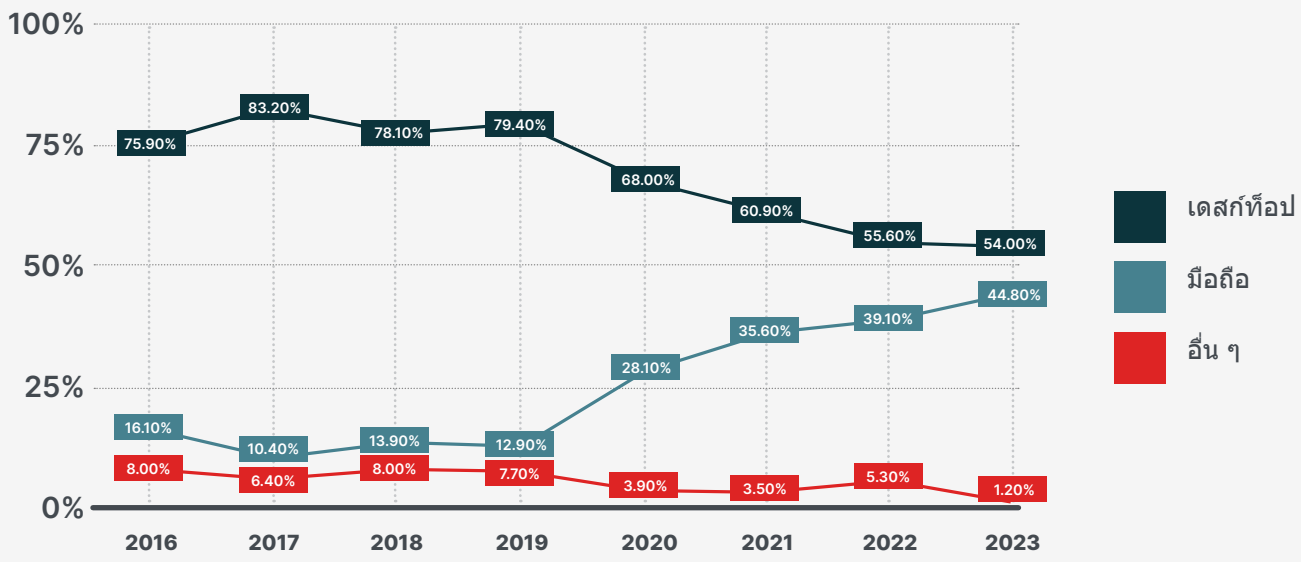
เปอร์เซ็นต์ของ Bad Bot ที่รายงานตนเองว่าเป็นเอเยนต์ผู้ใช้บนเดสก์ท็อป เช่น Chrome, Firefox, Safari หรือ Edge ลดลงจาก **68%** ในปี 2020 เป็น **54%** ในปี 2023

ส่วนที่เหลือของปริมาณการเข้าเยี่ยมชมของ Bad Bot **1.2%** ได้รายงานตนเองว่าเป็นเอเยนต์ของผู้ใช้รายอื่น (เช่น Playstation, Nintendo, Smart TV เป็นต้น)

**ประเภทเอเยนต์ผู้ใช้ Bad Bot ในปี 2023**




**ประเภทเอเยนต์ผู้ใช้ในที่ Bad Bot รายงานในปี 2016-2023**




7 https://explodingtopics.com/blog/mobile-internet-traffic

# การเพิ่มขึ้นของพร็อกซีที่อยู่อาศัย

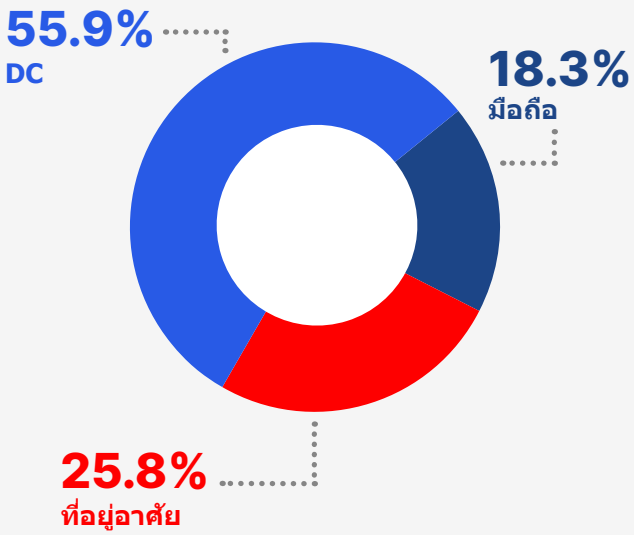
ในปีนี้ การเข้าเยี่ยมชมของ Bad Bot ที่มาจาก ISP ที่อยู่อาศัยมีสัดส่วนเป็น **25.8%** ของการเข้าเยี่ยมชมของ Bad Bot ทั้งหมด เพิ่มขึ้นจาก **17.4%** ในปีที่ผ่านมา แม้ว่าในอดีต การปลอมตัวเป็นผู้ใช้ที่เป็นมนุษย์โดยชอบด้วยกฎหมายโดยแสดงเป็นเอเยนต์ผู้ใช้ (เบราว์เซอร์) ที่ผู้ใช้ที่ถูกต้องตามกฎหมายใช้กันทั่วไปถือเป็นเทคนิคการหลีกเลี่ยงขั้นสูง แต่ปัจจุบันได้กลายเป็นสินค้าโภคภัณฑ์ไปแล้ว การซ่อนที่มาของคำขอโดยใช้พร็อกซีสำหรับมือถือหรือที่พักอาศัยจะช่วยเพิ่มมิติความน่าเชื่อถืออีกระดับหนึ่ง พฤติกรรมของบอทประเภทนี้จะสร้างความแตกต่างในแง่ประสงค์ร้ายอย่างซับซ้อน ต่อเนื่อง และมุ่งมั่น ด้วยวิธีการและความสามารถในการบรรลุเป้าหมายจากสิ่งที่มีความซับซ้อนน้อยกว่า

ทีมวิจัยภัยคุกคามของ Imperva พบว่าโปรแกรมเมอร์บอทใช้การรวมระบบพร็อกซี IP ที่อยู่อาศัยมากขึ้นภายในข้อเสนอซอฟต์แวร์ที่ได้รับการจัดการ (เช่น บอท All-in-One) และฐานความรู้การทำงานร่วมกัน เราได้พัฒนากลไกการตรวจจับแบบกำหนดเป้าหมายเพื่อตรวจจับและตอบโต้เทคนิคการหลบเลี่ยงนี้

แม้ว่าศูนย์ข้อมูลยังคงเป็นแหล่งที่มาของปริมาณการโจมตีของบอทส่วนใหญ่ **(55.9%)** การเข้าเยี่ยมชมที่มาจากช่องทางเหล่านี้ได้ลดลงในปีนี้ หลังจากที่เพิ่มขึ้นอย่างน่าประหลาดใจในปีที่ผ่านมา ในปี 2020 ศูนย์ข้อมูลมีสัดส่วน **54%** ของการเข้าเยี่ยมชมของ Bad Bot ลดลงเป็น **45.1%** ในปี 2021 จากนั้นก็เพิ่มขึ้นอย่างมากเป็น **58.6%** ของการเข้าเยี่ยมชมของ Bad Bot ทั้งหมดในปี 2022 อย่างไรก็ตามในปีนี้จำนวนของการโจมตีของบอทได้ลดลง

ปริมาณการเข้าเยี่ยมชมที่มาจาก ISP มือถือลดลงจาก **24.1%** ในปี 2022 เป็น **18.3%** ในปี 2023

**ปริมาณการเข้าเยี่ยมชมของ Bad Bot ตามประเภท ISP ในปี 2023**




## การเข้าเยี่ยมชมของ Bad Bot ที่มาจาก ISP มือถือและที่อยู่อาศัยมีสัดส่วนสูงที่สุด

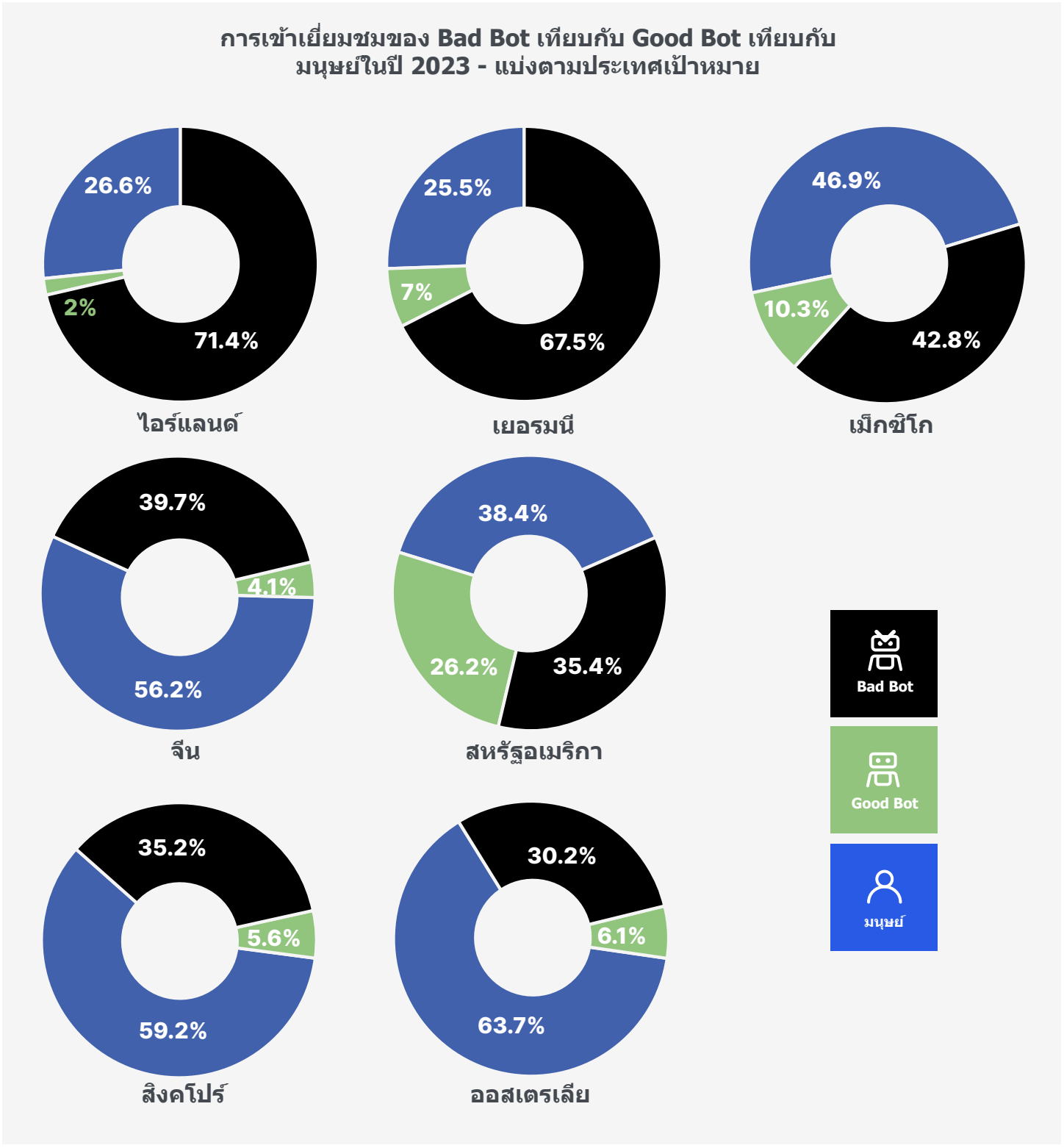
ตามที่เราเพิ่งจะอธิบายไป พร็อกซีมือถือและที่อยู่อาศัยได้รับความนิยมมากขึ้นในหมู่ผู้อยู่เบื้องหลัง Bad Bot China Telecom อยู่ในอันดับ 2 Comcast อยู่ในอันดับ 4 และ Spectrum อยู่ในอันดับ 6 อย่างไรก็ตาม Amazon ยังคงครองตำแหน่งอันดับหนึ่ง โดยมีปริมาณการเข้าเยี่ยมชมของบอทอยู่ที่ 17.01%

**ISP อันดับต้น ๆ ที่เป็นที่มาของ Bot**

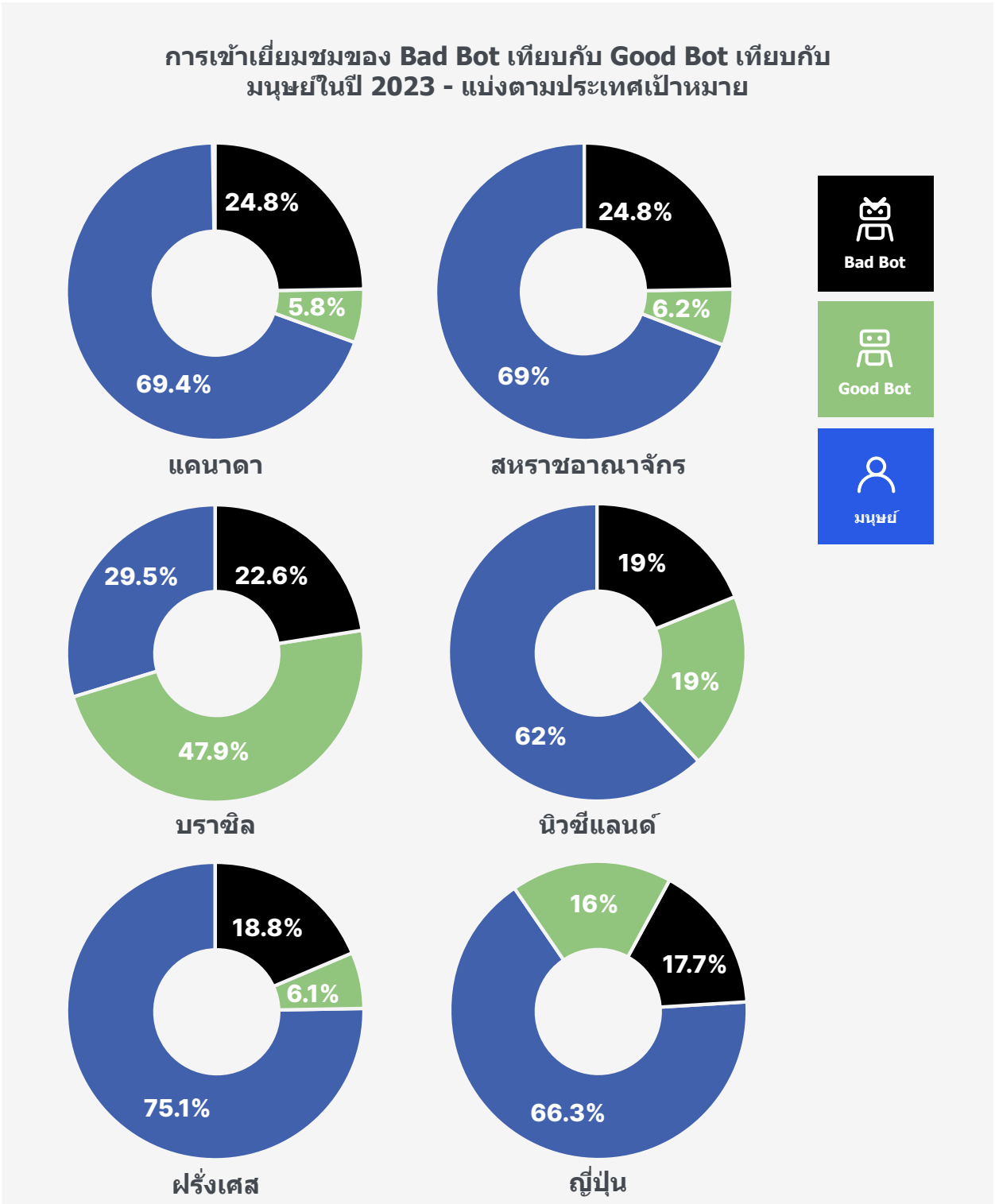
| ISP | % ของปริมาณการเข้าเยี่ยมชมของบอท |
|---|---|
| Amazon.com | 17.01% |
| China Telecom | 3.42% |
| Digital Ocean | 2.78% |
| Comcast Cable | 1.76% |
| Microsoft Azure | 1.63% |
| Spectrum | 1.60% |
| Safaricom | 1.51% |
| Google Cloud | 1.51% |
| Jio | 1.34% |
| Contabo GmbH | 0.99% |

# Bad Bot ทั่วโลก

การกระจายตัวของการเข้าเยี่ยมชมในประเทศชาติ เราได้สำรวจใน 13 ประเทศและพบว่า 6 จาก 13 ประเทศประสบปัญหาปริมาณการเข้าเยี่ยมชมของ Bad Bot สูงกว่าค่าเฉลี่ย ซึ่งเกินกว่าค่าเฉลี่ยทั่วโลกที่ **32%** ในปีนี้ เยอรมนีและไอร์แลนด์ทำสถิติใหม่อีกครั้งที่ **60%** ของการเข้าเยี่ยมชมมาจาก Bad Bot ในทำนองเดียวกัน สหรัฐอเมริกาพบว่ามีอัตราส่วนปริมาณการเข้าเยี่ยมชมของ Bad Bot สูงกว่าทั่วโลกเล็กน้อยที่ **35.4%** ของการเข้าเยี่ยมชมทั้งหมดที่เกิดจาก Bad Bot



## การเข้าเยี่ยมชมของ Bad Bot เทียบกับ Good Bot เทียบกับ มนุษย์ในปี 2023 - แบ่งตามประเทศเป้าหมาย



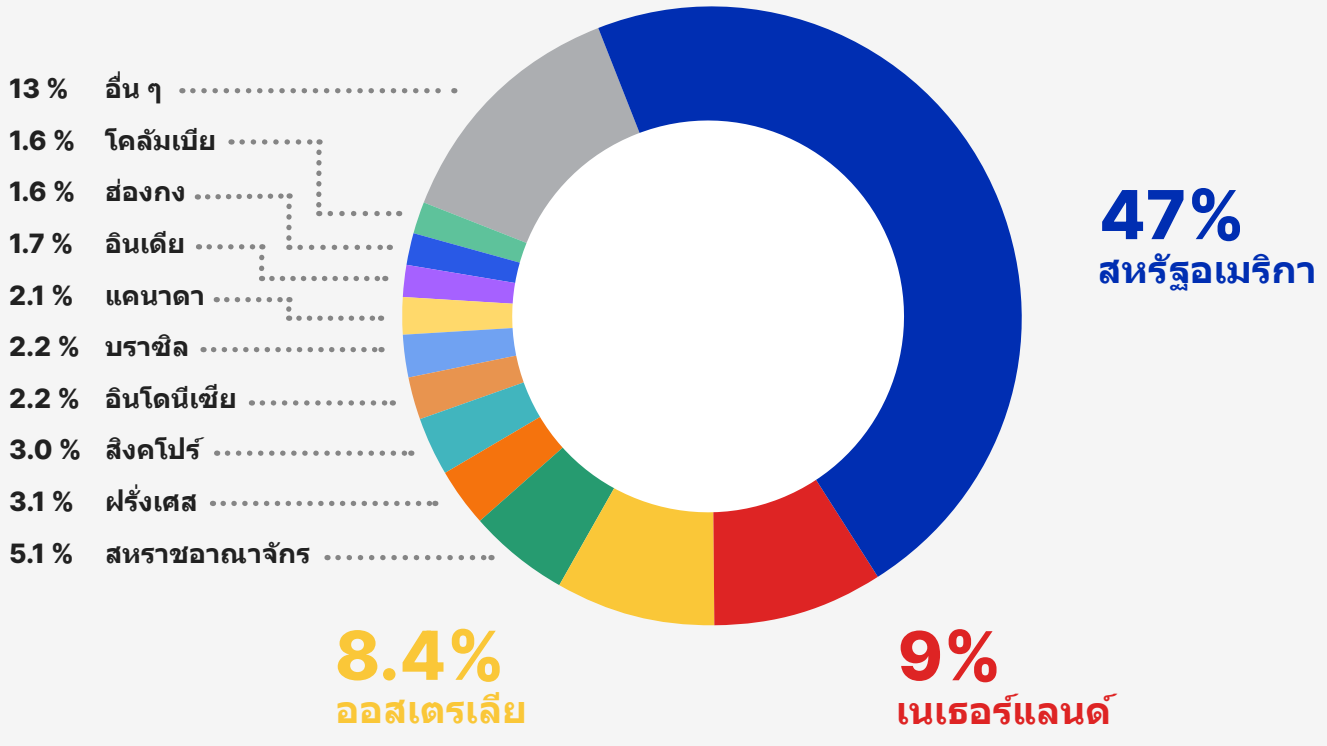
# สหรัฐอเมริกาและเนเธอร์แลนด์ตกเป็นเป้าของการโจมตีด้วยบอทมากที่สุด

การโจมตีของบอทยังคงมุ่งเป้าไปที่สหรัฐอเมริกา ซึ่งยังคงเป็นเป้าหมายที่สำคัญที่สุดด้วยสัดส่วน **47%** ของการโจมตีที่มุ่งตรงไปยังเว็บไซต์ในสหรัฐ เปอร์เซ็นต์นี้เพิ่มขึ้นเมื่อเทียบกับปีที่ผ่านมาที่ **41.1%** ของการโจมตีของบอทมุ่งเน้นไปที่สหรัฐอเมริกา เนเธอร์แลนด์แซงหน้าออสเตรเลียเล็กน้อยในปีนี้ โดยขึ้นสู่อันดับสองที่ **9%** ของการโจมตีของบอทโดยพุ่งเป้าไปที่ประเทศดังกล่าว ออสเตรเลียตกเป็นเป้าหมายที่ **8.4%** ของการโจมตีด้วยบอท ซึ่งมีสัดส่วนเกือบครึ่งหนึ่งของปีที่ผ่านมา **(16.4%)** แต่สอดคล้องกับข้อมูลอดีต **(6.8% ในปี 2021)** สหราชอาณาจักรเป็นประเทศที่ตกเป็นเป้าหมายมากเป็นอันดับสี่ที่ **5.1%** ของการโจมตี ตามมาด้วยฝรั่งเศสซึ่งตกเป็นเป้าหมายที่ **3.1%**

## 10 อันดับแรกของประเทศที่ถูกโจมตีโดย Bad Bot มากที่สุด

1. สหรัฐอเมริกา
2. เนเธอร์แลนด์
3. ออสเตรเลีย
4. สหราชอาณาจักร
5. ฝรั่งเศส
6. สิงคโปร์
7. อินโดนีเซีย
8. บราซิล
9. แคนาดา
10. อินเดีย

### การกระจายการโจมตีของบอทแยกตามประเทศเป้าหมาย (2023)



# Bad Bot ในยุคปัญญาประดิษฐ์



**การเพิ่มขึ้นของปัญญาประดิษฐ์ (AI) และโมเดลการเรียนรู้ขนาดใหญ่ (LLM) กำลังเปลี่ยนแปลงชีวิตของเราในหลาย ๆ ด้านเกินกว่าที่จะนับได้ นับตั้งแต่การยกระดับการดำเนินธุรกิจไปจนถึงการทำให้ชีวิตประจำวันของเราสะดวกสบายยิ่งขึ้น เทคโนโลยีเหล่านี้กำลังพลิกโฉมในหลาย ๆ ด้าน อย่างไรก็ตาม การเพิ่มขึ้นของ AI และ LLM ก็นำมาซึ่งความท้าทายมากมายเช่นกัน**

**เราได้กล่าวถึงผลกระทบระดับสูงของปัญหาต่อโปรไฟล์การเข้าชมอินเทอร์เน็ตตลอดทั้งรายงานมาแล้ว ผลกระทบเหล่านี้รวมไปถึงปริมาณการเข้าเยี่ยมชมอัตโนมัติที่เพิ่มขึ้น และความแตกต่างที่ชัดเจนระหว่าง Bad Bot แบบธรรมดาและขั้นสูง ทั้งหมดนี้ได้อธิบายอย่างครอบคลุมในบทสรุปผู้บริหาร แต่อย่างไรก็ดี ความท้าทายบางอย่างก็มีความซับซ้อนมากขึ้น เช่น การอภิปรายครั้งใหม่เกี่ยวกับความถูกต้องตามกฎหมายของการดูดข้อมูลจากเว็บ ซึ่งเป็นประเด็นที่ถกเถียงอย่างคุกรุ่นมานานหลายปี**

AI และ LLM ได้นำเอา**การดูดข้อมูลเว็บกลับมาเป็นประเด็นสำคัญอีกครั้ง**

การดูดข้อมูลจากเว็บ ซึ่งเป็นแนวปฏิบัติในการใช้บอทเพื่อดึงข้อมูลจากเว็บไซต์ไม่ใช่เรื่องใหม่ อย่างไรก็ตาม การถือกำเนิดขึ้นของ AI และ LLM ได้ทำให้ปัญหานี้กลับมาเป็นที่สนใจอีกครั้ง เทคโนโลยีขั้นสูงเหล่านี้อาศัยข้อมูลจำนวนมหาศาลสำหรับการฝึกสอน ซึ่งมักได้มาจากการดูดข้อมูลจากเว็บ แม้ว่าแนวปฏิบัตินี้สามารถกระตุ้นการพัฒนา AI ได้ แต่ก็ก่อให้เกิดข้อกังวลทางกฎหมายและจริยธรรมที่สำคัญ

ความถูกต้องตามกฎหมายของการดูดข้อมูลจากเว็บส่วนใหญ่ขึ้นอยู่กับเขตอำนาจศาลและสถานการณ์เฉพาะ อย่างไรก็ตาม การถือกำเนิดของ AI ทำให้เรื่องนี้ซับซ้อนยิ่งขึ้น แม้ว่าบางคนอาจจะแย้งว่าข้อมูลมีความจำเป็นสำหรับการพัฒนาเทคโนโลยี AI แต่บางคนก็แย้งว่าข้อมูลดังกล่าวละเมิดกฎหมายลิขสิทธิ์และสิทธิความเป็นส่วนตัว

ประเด็นหลักของการอภิปรายอยู่ที่การใช้เนื้อหาและข้อมูลที่เป็นกรรมสิทธิ์ในการฝึกสอนโมเดล AI หลายองค์กรโต้แย้งว่าสิทธิ์ในทรัพย์สินทางปัญญาของตนถูกละเมิดเมื่อข้อมูลของพวกเขาถูกคัดลอกโดยไม่ได้รับอนุญาต ในทางกลับกัน ผู้เสนอ Web Scraping แย้งว่าแนวปฏิบัติดังกล่าวมีความจำเป็นต่อการพัฒนาเทคโนโลยี AI และการเรียนรู้ของเครื่อง

การชักเย่อระหว่างนวัตกรรมและความเป็นส่วนตัวนี้นำไปสู่การถกเถียงครั้งใหม่เกี่ยวกับความถูกต้องตามกฎหมายของการดูดข้อมูลจากเว็บ กฎหมายที่ควบคุมแนวปฏิบัตินี้มักจะล้าสมัยและมีความแตกต่างกันอย่างมากในแต่ละประเทศ ทำให้เป็นปัญหาที่ซับซ้อน ในขณะที่ AI และ LLM มีการพัฒนาอย่างต่อเนื่อง จึงมีความจำเป็นเร่งด่วนในการปรับปรุงกฎหมายและกฎระเบียบเพื่อให้เกิดความสมดุลระหว่างการส่งเสริมความก้าวหน้าทางเทคโนโลยีและการปกป้องเนื้อหาและข้อมูลที่เป็นกรรมสิทธิ์

ในคดีทางกฎหมายที่เกิดเป็นครั้งแรก The New York Times ได้ยื่นฟ้อง OpenAI และ Microsoft โดยกล่าวหาว่าละเมิดลิขสิทธิ์จากการคัดลอกเว็บเพื่อฝึกโมเดล AI OpenAI โต้แย้งว่าการกระทำของตนได้รับการคุ้มครองภายใต้หลักการ "การใช้งานโดยชอบธรรม" ของกฎหมายลิขสิทธิ์ของสหรัฐอเมริกา ในขณะเดียวกัน The Times ยืนยันว่าการใช้เนื้อหาของ OpenAI ไม่เป็นไปตามเกณฑ์ "การเปลี่ยนแปลง" ที่จำเป็นสำหรับการใช้งานโดยชอบ ผลลัพธ์ของการฟ้องร้องนี้อาจเป็นตัวกำหนดขอบเขตของกฎหมายลิขสิทธิ์และ AI ใหม่ ซึ่งอาจกำหนดบรรทัดฐานสำหรับการใช้เนื้อหาที่มีลิขสิทธิ์ในการฝึกสอน AI ได้อย่างถูกต้องตามกฎหมาย นอกจากนี้ยังเน้นย้ำถึงความจำเป็นเร่งด่วนในการปรับปรุงกฎหมายลิขสิทธิ์ที่ทำให้เกิดความสมดุลระหว่างสิทธิ์ของผู้สร้างเนื้อหากับความต้องการของนวัตกรรม AI กรณีนี้ได้เน้นย้ำถึงความท้าทายทางกฎหมายและจริยธรรมที่ซับซ้อนซึ่งเกิดจากการดูดข้อมูลจากเว็บในยุคของ AI โดยเน้นย้ำถึงความจำเป็นสำหรับธุรกิจในการปกป้องทรัพย์สินดิจิทัลในเชิงรุก

ในขณะที่ AI ยังคงพัฒนาต่อไป ความจำเป็นในการมีแนวทางทางกฎหมายที่ชัดเจนซึ่งสมดุลระหว่างความต้องการข้อมูลที่เกี่ยวข้องกับกฎหมายลิขสิทธิ์และสิทธิความเป็นส่วนตัวจึงมีความสำคัญมากขึ้นกว่าที่ผ่านมา การถกเถียงกันจะยังคงมีขึ้นอีกยาวไกล และในขณะที่เราก้าวไปข้างหน้า ธุรกิจ ระบบกฎหมาย และผู้นำด้านเทคโนโลยีจะต้องก้าวผ่านภูมิทัศน์ที่ซับซ้อนนี้ด้วยความระมัดระวังและความรับผิดชอบ

# การจองร้านอาหารกลายเป็นความฮอตครั้งใหม่

มีกฎง่าย ๆ หรือสมการเกี่ยวกับ Scalping Bot: ความต้องการสูงบวกกับการมีให้ในจำนวนที่จำกัดเท่ากับความสนใจของ Bot ผู้อยู่เบื้องหลังบอทเหล่านี้เป็นคนที่ฉวยโอกาสสูงและจะใช้ประโยชน์จากสถานการณ์ใด ๆ ที่มีอุปทานต่ำและมีความต้องการสูง เรายังเห็นบอทขัดขวางการทำหนังสือเดินทาง วีซ่า และการนัดหมายสอบใบขับที่ทั่วโลก เนื่องจากมีงานในมือที่เกิดจากการแพร่ระบาดระหว่างปี 2020 ถึง 2022

ดังนั้นจึงไม่น่าแปลกใจที่ตอนนี้บอทได้พุ่งเป้าไปที่อุตสาหกรรมร้านอาหารโดยการจองร้านช่วงไพรม์ไทม์และขายในราคาที่สูงเกินไปบนแพลตฟอร์มของบุคคลที่สาม ในยุคดิจิทัลที่ความสะดวกสบายเป็นสิ่งสำคัญที่สุด การจองทางออนไลน์ได้กลายเป็นบรรทัดฐานในการได้ที่นั่งในร้านอาหารที่คุณชื่นชอบ

ลองนึกถึงภาพการวางแผนรับประทานอาหารค่ำมื้อพิเศษที่ร้านอาหารชั้นนำ เพียงเพื่อจะพบว่าที่นั่งว่างทั้งหมดหายไปภายในเสี้ยววินาทีหลังจากเปิดตัว ที่แย่ไปกว่านั้นก็คือ การจองเหล่านี้จะปรากฏบนแพลตฟอร์มการขายต่อในภายหลัง

**ความต้องการสูงบวกมีจำหน่ายอย่างจำกัด**

**=**

**ความสนใจของบอท**

บังคับให้คุณจ่ายเงินสูงถึง $340 เพื่อจองโต๊ะที่เปิดให้จองฟรีในตอนแรก นี่คือความจริงสำหรับนักชิมจำนวนมากในทุกวันนี้ ซึ่งเกิดจากกิจกรรมที่ชั่วร้ายของ Bad Bot

เช่นเดียวกับที่บอททำกับตั๋วคอนเสิร์ตและรองเท้าผ้าใบที่เป็นของสะสม บอทเหล่านี้ใช้ประโยชน์จากระบบเพื่อแสวงหากำไร ทำให้แทบจะเป็นไปไม่ได้เลยที่ลูกค้าจริงจะได้รับประกันการจองในสถานที่ยอดนิยม เรื่องนี้ไม่เพียงแต่ทำให้ลูกค้าหงุดหงิดเท่านั้น แต่ยังส่งผลเสียต่อธุรกิจร้านอาหารอีกด้วย เมื่อที่นั่งที่ถูกจองเต็มด้วยบอท ร้านอาหารจะสูญเสียรายได้ที่อาจเกิดขึ้นจากโต๊ะว่างและค่าธรรมเนียมการยกเลิกที่เรียกเก็บจากบัตรเครดิตที่ไม่ถูกต้อง

เพื่อเป็นการแก้ปัญหา ร้านอาหารและแพลตฟอร์มการจองต่างกำลังทำสงครามกับภัยคุกคามทางไซเบอร์เหล่านี้ พวกเขากำลังใช้มาตรการเพื่อตรวจจับและบล็อกกิจกรรมที่น่าสงสัย เช่น การจองจากบัญชีที่มีที่อยู่อีเมลที่สับสนหรือหมายเลขโทรศัพท์ที่ถูกตัดสาย บางแห่งถึงกับลดจำนวนการจองทางออนไลน์ โดยเลือกที่จะต้อนรับลูกค้าที่วอล์กอินมากขึ้นแทน

# การแสวงหากำไรจากตั๋วเพิ่มขึ้นอย่างรวดเร็วในยุคหลังการเกิดโรคระบาด

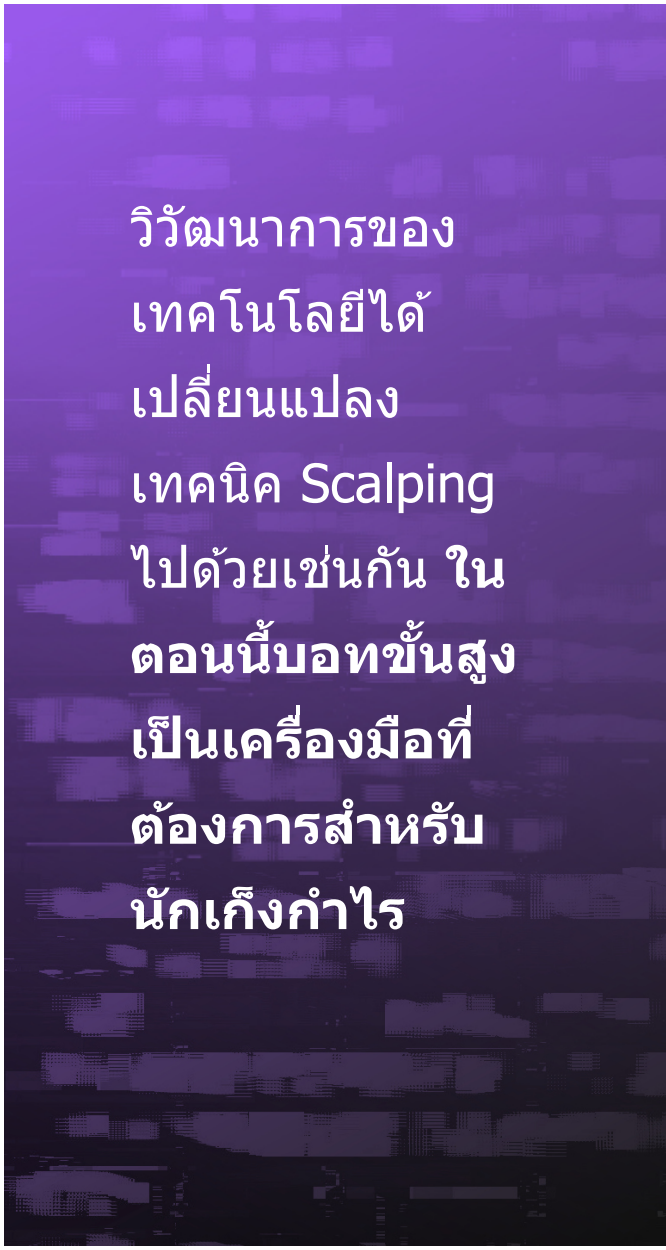
งานแสดงสดกลับมาอย่างยิ่งใหญ่ในช่วงสองสามปีที่ผ่านมา โดยมีความต้องการตั๋วคอนเสิร์ตทั่วโลกเพิ่มสูงขึ้นเป็นพิเศษ ตามที่กล่าวมาข้างต้น ความต้องการที่สูงบวกกับการนำเสนอในปริมาณที่จำกัดเท่ากับความสนใจของบอท อันที่จริง ได้มีการฟื้นตัวอย่างมากของการแสวงหากำไรจากตั๋ว (การซื้อตั๋วงานอีเวนต์จำนวนมากเพื่อขายต่อในราคาที่สูงเกินจริง) แนวปฏิบัติที่เก่าแก่นี้เป็นการดำเนินการโดยระบบอัตโนมัติในปัจจุบัน (หรือที่เรียกว่าบอท) ได้ค้นพบชีวิตใหม่ในยุคหลังการแพร่ระบาดของโรค

วิวัฒนาการของเทคโนโลยีได้เปลี่ยนแปลงเทคนิคการเทรดแบบ scalping โดยตอนนี้บอทขั้นสูงกลายเป็นเครื่องมือยอดนิยมสำหรับผู้เทรดแบบ scalping เว็บไซต์บันเทิงซึ่งจัดหมวดหมู่แพลตฟอร์มจำหน่ายตั๋ว พบว่ามีอัตราส่วนของ Bad Bot ขั้นสูงเป็นอันดับสองในปีที่ผ่านมาที่ **70.8%** (โปรดดูที่ส่วน "ความซับซ้อนของ Bad Bot ตามอุตสาหกรรม")

บอทเหล่านี้มักจะเป็น "โซลูชัน" แบบครบวงจร (AIO) ซึ่งช่วยให้ผู้อยู่เบื้องหลังสามารถดำเนินกระบวนการซื้อโดยอัตโนมัติได้ทั้งหมด พวกเขามักจะรวมเอาเทคนิคการหลีกเลี่ยงหลายอย่างและความสามารถในการแก้ไข CAPTCHA ประเด็นนี้ทำให้เกิดความไม่พอใจอย่างกว้างขวางในหมู่ผู้บริโภค และสร้างความท้าทายที่สำคัญสำหรับธุรกิจและอุตสาหกรรมบันเทิงสด

ธุรกิจต่างๆ เผชิญกับการสูญเสียรายได้ที่อาจเกิดขึ้น เนื่องจากลูกค้าที่แท้จริงไม่สามารถซื้อตั๋วในราคาหน้าตั๋วได้ ซึ่งเป็นการทำลายชื่อเสียงและความภักดีของลูกค้า ในทางกลับกัน ผู้บริโภคต้องต่อสู้กับราคาที่สูงเกินไปและการเข้าถึงงานกิจกรรมอย่างจำกัด ซึ่งนำไปสู่ความคับข้องใจและความไม่ไว้วางใจที่อาจเกิดขึ้นในตลาด

ความต้องการความบันเทิงสดที่เพิ่มขึ้นเนื่องจากข้อจำกัดในช่วงการแพร่ระบาดของโรคได้ผ่อนคลายลง ส่งผลให้เกิดการฟื้นตัวของการ Scalping ตั๋วเป็นเงาตามตัว เรื่องนี้ทำให้หลายประเทศต้องใช้มาตรการทางกฎหมายเพื่อต่อสู้กับปัญหานี้ อย่างไรก็ตาม เช่นเดียวกับความถูกต้องตามกฎหมายของการดูดข้อมูลจากเว็บ เป็นที่ชัดเจนแล้วว่าธุรกิจแทบจะรอไม่ไหวที่จะมีมาตรการทางกฎหมาย เนื่องจากพวกเขาต้องใช้มาตรการเชิงรุกเพื่อลดความเสี่ยงที่เกิดจากการเข้าเยี่ยมชมของบอท



# ข้อแนะนำ



ธุรกิจควรป้องกันตนเองจากบอทและการฉ้อโกงออนไลน์อย่างไร โซลูชันอเนกประสงค์อาจจะเข้าใจยาก เนื่องจากแต่ละเว็บไซต์มีช่องโหว่และเวกเตอร์การโจมตีเฉพาะตัว อย่างไรก็ตาม การใช้แนวทางเชิงรุกโดยใช้มาตรการรักษาความปลอดภัยหลายแง่มุมสามารถช่วยลดความเสี่ยงได้อย่างมาก ซึ่งรวมไปถึงการปรับใช้การตรวจจับบอทขั้นสูงและโซลูชันการจัดการความปลอดภัยทางไซเบอร์ กลยุทธ์เหล่านี้ร่วมกันสร้างกลไกการป้องกันที่ครอบคลุมต่อภูมิทัศน์ที่เปลี่ยนแปลงตลอดเวลาของการฉ้อโกงออนไลน์และภัยคุกคามในด้านความปลอดภัยที่เกี่ยวข้องกับบอท

## คำแนะนำเกี่ยวกับความปลอดภัยสำหรับการตรวจหากิจกรรม Bad Bot และการฉ้อโกงอัตโนมัติ

## 1. การระบุความเสี่ยง

**การหยุดการเข้าเยี่ยมชมของบอทเริ่มต้นด้วยการระบุความเสี่ยงที่อาจเกิดขึ้นกับเว็บไซต์ของคุณ:**

**A.** ความคิดริเริ่มในด้านการตลาดและอีคอมเมิร์ซมักจะดึงดูดบอทเพิ่มมากขึ้น โดยเฉพาะอย่างยิ่งในช่วงการเปิดตัวผลิตภัณฑ์ที่มีปริมาณจำกัดและมีความต้องการสูง ไม่ว่าจะเป็นรองเท้าผ้าใบรุ่นล่าสุด คอนโซลเกมยุคถัดไป หรือสินค้าสุดพิเศษสำหรับนักสะสม การระบุวันเปิดตัวสำหรับผลิตภัณฑ์ที่ปรารถนาเหล่านี้ถือเป็นสัญญาณสำหรับบอท หน่วยงานอัตโนมัติเหล่านี้มุ่งหวังที่จะทำให้ได้ครอบครองสินค้าก่อนที่ลูกค้าจริงจะสามารถทำได้ ซึ่งอาจผูกขาดการเข้าถึงและบ่อนทำลายความพยายามในการขายของคุณ สิ่งสำคัญก็คือต้องเสริมการป้องกันเว็บไซต์ของคุณเพื่อจัดการปริมาณการเข้าชมที่เพิ่มขึ้นอย่างมีประสิทธิภาพ เพื่อให้มั่นใจว่าคุณสามารถแยกแยะระหว่างผู้บริโภคที่ถูกกฎหมายและบอทหลบเลี่ยงที่มีเจตนาแย่งชิงการเปิดตัวผลิตภัณฑ์ได้ การใช้การวิเคราะห์การเข้าเยี่ยมชมขั้นสูง กลไกการตรวจจับบอทแบบเรียลไทม์ และมาตรการพิสูจน์ตัวตนที่มีประสิทธิภาพสามารถช่วยปกป้องแพลตฟอร์มของคุณได้ ทำให้มั่นใจได้ว่าลูกค้าจริงจะเข้าถึงได้อย่างยุติธรรม

**B.** การรับรู้ถึงช่องโหว่ที่อาจเกิดขึ้นบนเว็บไซต์ของคุณเป็นองค์ประกอบสำคัญของกลยุทธ์การจัดการบอทที่มีประสิทธิภาพ คุณสมบัติบางอย่างของเว็บไซต์มีความอ่อนไหวต่อกิจกรรมบอทที่เป็นอันตรายเป็นพิเศษ ตัวอย่างเช่น การรวมความสามารถในการเข้าสู่ระบบอาจนำไปสู่การโจมตี Credential Stuffing และ Credential Cracking ซึ่งผู้โจมตีใช้ข้อมูลประจำตัวที่ถูกขโมยเพื่อเข้าถึงโดยไม่ได้รับอนุญาต ในทำนองเดียวกัน การมีแบบฟอร์มชำระเงินอาจเพิ่มความเสี่ยงของการ

ฉ้อโกงบัตรเครดิต หรือที่เรียกว่า Carding หรือ Card Cracking นอกจากนี้ การใช้ฟังก์ชันบัตรของขวัญสามารถดึงดูดบอทที่มีเจตนาฉ้อโกงได้ เพื่อลดความเสี่ยงดังกล่าว จำเป็นต้องใช้มาตรการรักษาความปลอดภัยที่ได้รับการปรับปรุงและบังคับใช้กฎที่เข้มงวดมากขึ้นในหน้าเหล่านี้ การใช้การพิสูจน์ตัวตนแบบหลายปัจจัย CAPTCHA และการตรวจสอบกิจกรรมที่น่าสงสัยอย่างต่อเนื่องจะช่วยเพิ่มความแข็งแกร่งให้กับการป้องกันเว็บไซต์ของคุณจากภัยคุกคามอัตโนมัติเหล่านี้ได้อย่างมาก

# 2. การลดช่องโหว่

การรักษาความปลอดภัย API ที่เปิดเผยและแอปพลิเคชันมือถือมีความสำคัญพอ ๆ กับการปกป้องเว็บไซต์ของคุณ โดยเน้นย้ำถึงความจำเป็นสำหรับกลยุทธ์ความปลอดภัยทางไซเบอร์แบบองค์รวมที่ครอบคลุมจุดสัมผัสทางดิจิทัลทั้งหมด ต้องใช้มากกว่าการมุ่งเน้นไปที่ความปลอดภัยของเว็บไซต์ของคุณ API และแอปมือถือมักจะทำหน้าที่เป็นเกตเวย์ไปยังเว็บแอปพลิเคชันและข้อมูลที่ละเอียดอ่อนของคุณ โดยนำเสนอเวกเตอร์เพิ่มเติมสำหรับภัยคุกคามทางไซเบอร์ การใช้มาตรการรักษาความปลอดภัยที่แข็งแกร่งบนแพลตฟอร์มเหล่านี้และการบล็อกระหว่างระบบถือเป็นเรื่องที่สำคัญในการลดความเสี่ยง วิธีการที่ครอบคลุมนี้ช่วยให้มั่นใจได้ถึงกลไกการป้องกันที่ครบวงจรต่อการโจมตีที่อาจเกิดขึ้น ลดความเสี่ยงในการเข้าถึงแอปพลิเคชันเว็บและข้อมูลสำคัญของคุณโดยไม่ได้รับอนุญาตผ่านจุดเข้าใช้งานดิจิทัล

# 3. การลดภัยคุกคาม: เอเยนต์ผู้ใช้

เครื่องมือและสคริปต์บอทจำนวนมากมีสตริงเอเยนต์ผู้ใช้ที่มีเบราว์เซอร์เวอร์ชันล้าสมัย ในทางตรงกันข้าม มนุษย์ถูกบังคับให้อัปเดตเบราว์เซอร์ของตนเป็นเวอร์ชันใหม่โดยอัตโนมัติ ทำตามขั้นตอนเพื่อบล็อกเบราว์เซอร์เวอร์ชันที่ล้าสมัย:

| | **บล็อก**<br>สิ้นสุดระยะเวลาการใช้งานนานกว่าสามปี | **CAPTCHA**<br>สิ้นสุดระยะเวลาการใช้งานนานกว่าสองปี |
|---|---|---|
| **เวอร์ชันของ Chrome** | <95 | <105 |
| **เวอร์ชันของ Firefox** | <95 | <105 |
| **เวอร์ชันของ Safari** | <13 | <14 |
| **เวอร์ชันของ Internet Explorer** | <11 | <11 |

# 4. การลดภัยคุกคาม: พร็อกซี

การใช้บริการพร็อกซีโดยบอทที่เป็นอันตรายเพื่อปิดบังกิจกรรมของบอทมีเพิ่มมากขึ้น เนื่องจากผู้โจมตีใช้บริการเหล่านี้เพื่อจำลองพฤติกรรมที่ถูกต้องของผู้ใช้ ด้วยการใช้ประโยชน์จากการหมุนเวียน IP จากบริการ IP แบบกลุ่ม บอทสามารถที่จะปกปิดต้นกำเนิดที่แท้จริงได้ และทำให้ความพยายามในการตรวจจับซับซ้อนขึ้น แนวทางเชิงกลยุทธ์ในการบรรเทาภัยคุกคามนี้เกี่ยวข้องกับการจำกัดการเข้าถึงจากศูนย์ข้อมูล IP จำนวนมากที่รู้จัก ซึ่งจะช่วยลดโอกาสที่การเข้าเยี่ยมชมที่บอทเน็ตจะแทรกซึมเครือข่ายของคุณลงอย่างมาก แหล่งที่มาของการโจมตีผ่านพร็อกซีที่โดดเด่น รวมไปถึง ศูนย์ข้อมูลและผู้ให้บริการระบบคลาวด์ เช่น Host Europe GmbH, Dedibox SAS, Digital Ocean, OVH SAS และ Choopa, LLC การใช้การควบคุมการเข้าถึงและการตรวจสอบการเข้าเยี่ยมชมที่มาจากเอนทิตีเหล่านี้สามารถปรับปรุงสถานะความปลอดภัยของคุณได้โดยการระบุและบล็อกการเข้าเยี่ยมชมที่สร้างจากบอทล่วงหน้า ซึ่งจะช่วยลดความเสี่ยงที่เกี่ยวข้องกับการโจมตีที่เปิดใช้งานพร็อกซีเหล่านี้

# 5. การลดภัยคุกคาม: ระบบอัตโนมัติ

เครื่องมือสมัยใหม่ เช่น Puppeteer, Selenium และ WebDriver มักถูกใช้ในทางที่ผิดโดยผู้โจมตีเพื่อเลียนแบบการกระทำทางออนไลน์ของมนุษย์ ทำให้พวกเขาสามารถดำเนินกิจกรรมที่เป็นอันตราย เช่น การลงทะเบียนบัญชีจำนวนมาก และการขโมยข้อมูลได้ การแยกแยะความพยายามที่เป็นอันตรายเหล่านี้จากการเข้าเยี่ยมชมที่ถูกต้องนั้นจำเป็นต้องใช้กลยุทธ์การตรวจจับสัญญาณของระบบอัตโนมัติ เช่น การมีปฏิสัมพันธ์ที่รวดเร็วผิดปกติหรือรูปแบบการสืบค้นที่ผิดปกติ ด้วยการมุ่งเน้นพฤติกรรมเหล่านี้ องค์กรต่าง ๆ จึงสามารถตรวจจับและหยุดการโจมตีอัตโนมัติได้อย่างมีประสิทธิภาพ ปกป้องการมีปฏิสัมพันธ์ของผู้ใช้อย่างแท้จริง

# 6. ประเมินการเข้าชม

**A.** การระบุปริมาณการเข้าเยี่ยมชมของบอทโดยไม่มีตัวบ่งชี้ที่ชัดเจนทำให้เกิดความท้าทาย แต่รูปแบบเฉพาะมักบอกเป็นนัยถึงปริมาณการใช้งานเหล่านั้น อัตราการกลับออกไปสูงและอัตราคอนเวอร์ชันต่ำอาจเป็นสัญญาณบ่งบอกถึงการเข้าชมที่ไม่ใช่จากมนุษย์ นอกจากนี้ ปริมาณการเข้าเยี่ยมชมที่เพิ่มขึ้นอย่างกะทันหันโดยไม่ทราบสาเหตุหรือจำนวนคำขอที่สูงผิดปกติซึ่งพุ่งเป้าไปที่ URL เฉพาะมักส่งสัญญาณถึงกิจกรรมของบอท การตรวจสอบความผิดปกติเหล่านี้ช่วยให้องค์กรสามารถตั้งค่าสถานะการเข้าเยี่ยมชมของบอทได้ อำนวยความสะดวกในการตรวจสอบเพิ่มเติม และมาตรการตอบสนองที่เหมาะสมเพื่อลดการแทรกแซงที่ไม่พึงประสงค์

**B.** การเข้าเยี่ยมชมที่เพิ่มขึ้นอย่างกะทันหันไปยังจุดสิ้นสุดเฉพาะอาจบ่งชี้ว่าบอทกำหนดเป้าหมายไปที่เหตุการณ์หรือการดำเนินการเฉพาะ เพื่อประเมินว่าการเพิ่มขึ้นอย่างรวดเร็วนี้เกิดจากบอทหรือไม่ ให้วิเคราะห์แหล่งที่มาของการเข้าชมที่เพิ่มขึ้นนี้ มองหารูปแบบ เช่น ที่อยู่ IP เดียว, ISP หรือ URL เฉพาะที่สร้างระดับการเข้าเยี่ยมชมที่สูงกว่าปกติอย่างมาก การระบุแหล่งที่มาเหล่านี้สามารถให้หลักฐานที่ชัดเจนเกี่ยวกับกิจกรรมของบอท ช่วยให้คุณสามารถดำเนินการตามเป้า

หมายได้ ตัวอย่างเช่น หากการเข้าเยี่ยมชมส่วนใหญ่มาจาก IP เดียวหรือช่วง IP ที่แคบ ก็ถือเป็นตัวบ่งชี้ที่ชัดเจนถึงความพยายามในการเข้าถึงอัตโนมัติ ข้อมูลเชิงลึกดังกล่าวมีความสำคัญอย่างยิ่งในการปรับใช้มาตรการตอบโต้ที่มีประสิทธิภาพต่อการโจมตีของบอท เพื่อให้มั่นใจว่าสินทรัพย์ดิจิทัลของคุณจะยังคงได้รับการปกป้อง

# 7. ตรวจสอบการเข้าเยี่ยมชม

**A.** กำหนดพื้นฐานความพยายามเข้าสู่ระบบที่ล้มเหลวในหน้าเข้าสู่ระบบ จากนั้นตรวจสอบความผิดปกติหรือการเพิ่มขึ้นอย่างรวดเร็ว ตั้งค่าการแจ้งเตือนเพื่อให้คุณได้รับแจ้งโดยอัตโนมัติหากมีเหตุการณ์เกิดขึ้น การโจมตีขั้นสูงที่มีปริมาณ "ต่ำและช้า" จะไม่กระตุ้นการแจ้งเตือนผู้ใช้หรือระดับเซสชัน ดังนั้นอย่าลืมตั้งค่าเกณฑ์ทั่วโลก

**B.** ในหน้าชำระเงินและการพิสูจน์ตัวตนของบัตรของขวัญ ความล้มเหลวที่เพิ่มขึ้น หรือแม้แต่การเข้าเยี่ยมชม อาจเป็นสัญญาณของการโจมตีด้วยการสร้างบัตร หรือบอท เช่น GiftGhostBot กำลังพยายามขโมยยอดคงเหลือของบัตรของขวัญ

# 8. การรับรู้

การรักษาความระมัดระวังเกี่ยวกับการละเมิดและการรั่วไหลของข้อมูลทั่วโลกถือเป็นเรื่องที่สำคัญ ความธรรมดาที่ผู้โจมตีสามารถซื้อข้อมูลประจำตัวจากการละเมิดเหล่านี้หรือเช่าโครงสร้างพื้นฐานของบอทเพื่อทำการโจมตีอัตโนมัติจะยกระดับภัยคุกคามให้กลายเป็นความเสี่ยงที่จับต้องได้ บอทมักใช้ประโยชน์จากข้อมูลประจำตัวที่ถูกบุกรุกใหม่เพื่อทำการโจมตีแบบกรอกข้อมูลและเข้าครอบครองบัญชี (ATO) เนื่องจากข้อมูลประจำตัวเหล่านี้มีแนวโน้มที่จะยังคงใช้ได้อยู่ กลยุทธ์นี้เพิ่มโอกาสอย่างมากในการละเมิดบัญชีผู้ใช้บนแพลตฟอร์มของคุณ การรับทราบข้อมูลเกี่ยวกับการละเมิดดังกล่าวและการทำความเข้าใจผลกระทบของการละเมิดดังกล่าวสามารถช่วยให้คุณเสริมสร้างการป้องกันของคุณในเชิงรุก ลดโอกาสที่เว็บไซต์ของคุณจะกลายเป็นเป้าหมายของภัยคุกคามอัตโนมัติเหล่านี้

# 9. ประเมินโซลูชันการป้องกันบอท

การประเมินโซลูชันการป้องกันบอทถือเป็นเรื่องที่สำคัญ เนื่องจากภาพรวมของการโจมตีจากบอทได้เปลี่ยนแปลงไปอย่างมาก มาตรการง่าย ๆ ที่ครั้งหนึ่งเคยเพียงพอในการป้องกันบอทที่เป็นอันตรายกลับไม่มีประสิทธิภาพในปัจจุบัน ข้อมูลเชิงลึกที่รวบรวมไว้ในรายงานนี้เน้นย้ำว่าความซับซ้อนและความสามารถในการปรับตัวของบอทสมัยใหม่นั้นเหนือกว่าระดับก่อนหน้านี้ โดยที่ใช้งานง่ายและมีประสิทธิผล ทำให้บอทเหล่านี้กลายเป็นเครื่องมือที่อาชญากรไซเบอร์ชื่นชอบ บอทเหล่านี้พัฒนาอย่างรวดเร็ว ทำให้วิธีการตรวจจับแบบเดิมล้าสมัย และยังเลียนแบบพฤติกรรมของมนุษย์อย่างใกล้ชิดมากขึ้นกว่าเดิม ทำให้การแยกความแตกต่างระหว่างบอทเหล่านี้จากผู้ใช้ที่ถูก

ต้องเป็นเรื่องยาก ในสภาพแวดล้อมนี้ ซึ่งผู้โจมตีใช้ประโยชน์จากบอทเพื่อให้ได้รับผลลัพธ์สูงและผลประโยชน์ที่มีความเสี่ยงต่ำ การพยายามตอบโต้ภัยคุกคามเหล่านี้เพียงลำพังแทบจะเป็นไปไม่ได้เลย

ความจำเป็นในการใช้กลยุทธ์การป้องกันแบบไดนามิกนั้นมีความกดดันมากกว่าที่เคย เพราะไม่ใช่แค่การระบุบอทที่เป็นอันตรายเท่านั้น แต่ยังเกี่ยวข้องกับการแยกแยะความแตกต่างของบอทจากสิ่งที่มีประโยชน์ท่ามกลางความซับซ้อนที่เพิ่มขึ้น โซลูชันการป้องกันบอทที่ครอบคลุมควรรวมไปถึงแนวทางการป้องกันแบบหลายชั้น โดยควรรวมไปถึงการวิเคราะห์พฤติกรรมผู้ใช้ การทำโปรไฟล์ และการพิมพ์ลายนิ้วมือ กลยุทธ์นี้ไม่เพียงรักษาข้อดีของบอทที่ถูกกฎหมายเท่านั้น แต่ยังกรองกิจกรรมที่เป็นอันตรายออกได้อย่างมีประสิทธิภาพอีกด้วย แนวทางที่เหมาะสมอย่างยิ่งดังกล่าวต้องอาศัยความเชี่ยวชาญของทีมงานเฉพาะที่สามารถพัฒนาการป้องกันของคุณให้ทันกับภัยคุกคามที่เกิดขึ้นใหม่ ๆ ด้วย

# กรณีการใช้งาน Bad Bot

| ปัญหา Bad Bot | คำนิยาม | ส่งผลเสียต่อธุรกิจอย่างไร | อาการ | อุตสาหกรรมที่ตกเป็นเป้าหมาย |
|---|---|---|---|---|
| **การดูดข้อมูลราคา** | การใช้บอทเพื่อตรวจสอบและติดตามข้อมูลราคาอย่างผิดกฎหมาย โดยทั่วไปเพื่อตัดราคาคู่แข่งและเพิ่มยอดขาย | การสูญเสียยอดขายให้กับคู่แข่งที่ดูดข้อมูลราคาของคุณ ตัดราคา และเอาชนะคุณในตลาด<br><br>ชื่อเสียงที่เสียหายเนื่องจากข้อมูลที่คัดลอกมาถูกใช้ในลักษณะที่แสดงราคาหรือผลิตภัณฑ์ของธุรกิจอย่างไม่ถูกต้อง<br><br>มูลค่าตลอดชีวิตของลูกค้าแย่ลง<br><br>ส่งผลกระทบต่อประสิทธิภาพของเว็บไซต์ | อัตราคอนเวอร์ชันลดลง<br><br>อันดับ SEO ของคุณลดลง<br><br>การชะลอตัวและการหยุดทำงานของเว็บไซต์โดยไม่ทราบสาเหตุ (มักเกิดจากโปรแกรมดูดข้อมูลที่รุกราน) | ธุรกิจทั้งหมดที่แสดงราคา:<br>• ขายปลีก<br>• เกม<br>• สายการบิน<br>• การท่องเที่ยว |
| **การดูดข้อมูลเนื้อหา** | การใช้บอทเพื่อดึงเนื้อหาและข้อมูลจากเว็บไซต์ | การสูญเสียรายได้เนื่องจากการเผยแพร่เนื้อหาหรือข้อมูลธุรกิจของคุณที่อื่น ส่งผลให้มีผู้เยี่ยมชมเว็บไซต์ดั้งเดิมหรือซื้อผลิตภัณฑ์หรือบริการของคุณน้อยลง<br><br>เนื้อหาที่ซ้ำกันจะทำให้อันดับ SEO ของคุณได้รับความเสียหาย<br><br>ความเสียหายต่อชื่อเสียงของแบรนด์<br><br>ส่งผลกระทบต่อประสิทธิภาพของเว็บไซต์ | เนื้อหาของคุณปรากฏบนเว็บไซต์อื่น<br><br>อันดับ SEO ของคุณลดลง<br><br>การชะลอตัวและการหยุดทำงานของเว็บไซต์โดยไม่ทราบสาเหตุ (มักเกิดจากโปรแกรมดูดข้อมูลที่รุกราน) | คล้ายกับการดูดข้อมูลราคา แต่เพิ่มเติม:<br>• บอร์ดงาน<br>• โฆษณาย่อย<br>• ตลาด<br>• การเงิน<br>• การออกตั๋ว |
| **การเข้าควบคุมบัญชี** *(เช่น การกรอกข้อมูลประจำตัว การแคร็กข้อมูลประจำตัว)* | การใช้บอทเพื่อเข้าถึงบัญชีผู้ใช้ที่เป็นของบุคคลอื่นอย่างผิดกฎหมาย<br><br>โดยปกติแล้วจะทำได้โดยใช้เทคนิคการเข้าสู่ระบบแบบ Brute Force เช่น Credential Stuffing หรือ Credential Cracking | ผลกระทบโดยตรงต่อความภักดีและชื่อเสียงของแบรนด์ PR ในเชิงลบ<br><br>ลูกค้าหงุดหงิดเนื่องจากการล็อกบัญชี การโจรกรรมข้อมูล หรือการฉ้อโกงที่เพิ่มมากขึ้น<br><br>ส่งผลกระทบต่อประสิทธิภาพ ความพร้อมใช้งาน และความน่าเชื่อถือของเว็บไซต์<br><br>ความเสี่ยงจากการไม่ปฏิบัติตามกฎระเบียบความเป็นส่วนตัวของข้อมูล<br><br>ค่าใช้จ่ายในการสนับสนุนและการฉ้อโกงเพิ่มขึ้น | เพิ่มอัตราการเข้าสู่ระบบที่ล้มเหลว<br><br>เพิ่มการล็อคบัญชีลูกค้าและตั๋วบริการลูกค้า<br><br>การฉ้อโกงเพิ่มขึ้น (คะแนนสะสมที่หายไป บัตรเครดิตที่ถูกขโมย การซื้อที่ไม่ได้รับอนุญาต)<br><br>การปฏิเสธการชำระเงินเพิ่มขึ้น | ธุรกิจใด ๆ ที่มีหน้าเข้าสู่ระบบ |

| ปัญหา Bad Bot | คำนิยาม | ส่งผลเสียต่อธุรกิจอย่างไร | อาการ | อุตสาหกรรมที่ตกเป็นเป้าหมาย |
|---|---|---|---|---|
| **การสร้างบัญชี** *(หรือที่เรียกว่าการรวมบัญชี การฉ้อโกงบัญชีใหม่)* | การใช้บอทเพื่อสร้างบัญชีจำนวนมากโดยอัตโนมัติ บัญชีเหล่านี้สามารถนำไปใช้ในทางที่ผิดเพื่อทำการฉ้อโกงเนื้อหาสแปม หรือเผยแพร่โฆษณาชวนเชื่อในรูปแบบต่าง ๆ | ลดความน่าเชื่อถือของบางแพลตฟอร์มและเว็บไซต์ต่อบัญชีบอทที่ใช้ในการสแปมข้อความหรือขยายการโฆษณาชวนเชื่อ<br><br>การสูญเสียรายได้ให้กับบอทที่ใช้ประโยชน์จากเครดิตส่งเสริมการขายกับบัญชีใหม่ (เงิน คะแนน การเล่นฟรี)<br><br>การวัดตามจำนวนบัญชีผู้ใช้หรือการมีปฏิสัมพันธ์บนโซเชียลมีเดียที่เกิดจากบอทอาจนำไปสู่การตัดสินใจที่ไม่ดี | เพิ่มขึ้นอย่างผิดปกติในการสร้างบัญชีใหม่<br><br>สแปมความคิดเห็นที่เพิ่มขึ้น<br><br>อัตราคอนเวอร์ชันจากบัญชีใหม่ไปสู่ลูกค้าที่ชำระเงินลดลง | แพลตฟอร์มการส่งข้อความ<br>• โซเชียลมีเดีย<br>• เว็บไซต์ชุมชนการหาคู่<br><br>การละเมิดการโปรโมทการลงทะเบียน<br>• เกม<br>• การเงิน |
| **การฉ้อโกงบัตรเครดิต** *(หรือที่เรียกว่าCarding, การแคร็กการ์ด)* | การใช้บอทเพื่อตรวจสอบความถูกต้องของหมายเลขบัตรเครดิตที่ถูกขโมยจำนวนมาก หรือคาดเดารายละเอียดที่ขาดหายไป (CVV, วันหมดอายุ ฯลฯ) | การสูญเสียทางการเงินอันเนื่องมาจากความรับผิดของธุรกิจสำหรับกิจกรรมฉ้อโกงใด ๆ ที่เกิดขึ้นบนแพลตฟอร์มของตนเอง: จากการปฏิเสธการชำระเงินที่มีราคาแพงไปจนถึงการสูญเสียรายได้เนื่องจากความไว้วางใจของผู้บริโภคลดลง<br><br>ชื่อเสียงของแบรนด์เสียหาย<br><br>ค่าเสียหายจากการฉ้อโกงของกิจการ<br><br>เพิ่มค่าใช้จ่ายในการบริการลูกค้าเพื่อดำเนินการปฏิเสธการชำระเงินที่ฉ้อโกง<br><br>การไม่ปฏิบัติตามกฎระเบียบความเป็นส่วนตัวของข้อมูล (PCI-DSS, GDPR ฯลฯ) | การฉ้อโกงบัตรเครดิตเพิ่มขึ้น<br><br>เพิ่มการโทรสนับสนุนลูกค้า<br><br>มีการประมวลผลการปฏิเสธการชำระเงินที่เพิ่มขึ้น | เว็บไซต์ใด ๆ ที่มีตัวประมวลผลการชำระเงิน:<br>• ขายปลีก<br>• องค์กรไม่แสวงผลกำไร/องค์กรการกุศล<br>• สายการบิน<br>• การท่องเที่ยว<br>• การออกตั๋ว<br>• การเงิน<br>• เกม |
| **การปฏิเสธการให้บริการ** | การใช้บอทเพื่อครอบงำเว็บไซต์ด้วยการส่งคำขอส่งผลให้ทรัพยากร เช่น ระบบไฟล์ หน่วยความจำ กระบวนการ เธรด CPU และทรัพยากรบุคคล หรือทางการเงินถูกใช้จนหมดไป | ทำให้ประสิทธิภาพเว็บไซต์ช้าลง ทำให้เกินความสามารถหรือหยุดทำงาน<br><br>สูญเสียรายได้จากการไม่พร้อมใช้งานของเว็บไซต์<br><br>ชื่อเสียงของแบรนด์เสียหาย<br><br>ลูกค้าที่มีศักยภาพจะปั่นป่วน | การเข้าชมที่เพิ่มขึ้นอย่างผิดปกติและไม่สามารถอธิบายได้บนแหล่งข้อมูลเฉพาะ (การเข้าสู่ระบบ การสมัครหน้าผลิตภัณฑ์ ฯลฯ)<br><br>การร้องเรียนการบริการลูกค้าเพิ่มขึ้น | ทุกอุตสาหกรรม |
| **การตรวจสอบยอดคงเหลือของบัตรของขวัญและการใช้ในทางที่ผิด** | การใช้บอทเพื่อทำการแจงนับหมายเลขบัตรของขวัญที่เป็นไปได้โดยอัตโนมัติเทียบกับหน้าการตรวจสอบยอดคงเหลือเพื่อขโมยยอดคงเหลือในบัตรของขวัญ | เช่นเดียวกับการฉ้อโกงบัตรเครดิต การฉ้อโกงบัตรของขวัญนำไปสู่การสูญเสียขั้นสุดท้ายเนื่องจากบอทที่ขโมยเงินจากบัตรของขวัญ<br><br>เพิ่มค่าใช้จ่ายในการบริการลูกค้าเพื่อดำเนินการปฏิเสธการชำระเงินที่ฉ้อโกง<br><br>มีชื่อเสียงไม่ดีในสายตาของลูกค้าและการสูญเสียยอดขายในอนาคต | การส่งคำขอที่เพิ่มขึ้นอย่างรวดเร็วไปยังหน้ายอดคงเหลือของบัตรของขวัญ<br><br>การโทรติดต่อฝ่ายบริการลูกค้าเพิ่มขึ้นเกี่ยวกับยอดคงเหลือที่หายไป | ธุรกิจใด ๆ ที่เสนอบัตรของขวัญเป็นตัวเลือกในการชำระเงิน<br>- ขายปลีกเป็นหลัก |

| ปัญหา Bad Bot | คำนิยาม | ส่งผลเสียต่อธุรกิจอย่างไร | อาการ | อุตสาหกรรมที่ตกเป็นเป้าหมาย |
|---|---|---|---|---|
| **การปฏิเสธสินค้าในสต็อก** | การใช้บอทเพื่อเก็บสินค้าไว้ในตะกร้าสินค้าโดยไม่เคยทำการซื้อจนเสร็จสิ้น ถือเป็นการปฏิเสธผู้บริโภคที่ถูกต้อง | การสูญเสียรายได้จากการไม่สามารถขายสินค้าได้เพราะถูกเก็บไว้ในตะกร้าสินค้าโดยบอท<br><br>อัตราคอนเวอร์ชันที่ลดลง<br><br>เพิ่มอัตราการละทิ้งรถเข็น<br><br>ชื่อเสียงเสียหายในสายตาของลูกค้าเนื่องจากพ่อค้าคนกลางไร้ยางอายจะถือครองสินค้าคงคลังไว้ทั้งหมดจนกว่าจะนำไปขายต่อที่อื่น | มีสิ่งที่ถูกทิ้งในตะกร้าช้อปปิ้งเพิ่มขึ้น<br><br>อัตราคอนเวอร์ชันลดลง<br><br>ได้รับข้อร้องเรียนจากลูกค้าเพิ่มขึ้นเกี่ยวกับการขาดสินค้าในสต็อก | ธุรกิจที่นำเสนอสินค้าที่หายากหรือมีความละเอียดอ่อนต่อเวลา:<br>• สายการบิน<br>• ตั๋ว<br>• ขายปลีก<br>• การดูแลสุขภาพ |
| **Scalping** | การใช้บอทเพื่อให้ได้เปรียบอย่างไม่เป็นธรรมเหนือผู้บริโภคที่ถูกต้องเหมาะสม และได้รับในสิ่งที่นำเสนอในแบบจำกัดและ/หรือสินค้า/บริการที่เป็นที่ต้องการสูง | ทำให้ชื่อเสียงของลูกค้าเสียหาย<br><br>ทำให้ประสิทธิภาพของเว็บไซต์ช้าลง ทำให้ประสิทธิภาพการทำงานลดลงหรือหยุดทำงาน ส่งผลให้สูญเสียรายได้<br><br>มูลค่าอายุการใช้งาน (LTV) ต่ำลง เนื่องจากบอทจะไม่กลับมาหารายการเพิ่มเติมเป็นประจำ<br><br>มูลค่าตะกร้าเฉลี่ย (ABV) ต่ำลง เนื่องจากบอทพุ่งเป้าไปที่ผลิตภัณฑ์เดียวซึ่งตรงข้ามกับผู้บริโภคที่ถูกต้องเหมาะสมซึ่งมีแนวโน้มที่จะซื้อสินค้าเพิ่มเติม | การชะลอตัวและการหยุดทำงานของเว็บไซต์โดยไม่มีคำอธิบาย (มักเกิดจากบอทดูดข้อมูลที่รุกราน)<br><br>อัตราคอนเวอร์ชันลดลง<br><br>ได้รับข้อร้องเรียนของลูกค้าเพิ่มขึ้นเกี่ยวกับการขาดสินค้าในสต็อก | คล้ายกับการปฏิเสธสินค้าในสต็อก:<br>• สายการบิน<br>• ตั๋ว<br>• ขายปลีก<br>เช่น รองเท้าผ้าใบ คอนโซล ฮาร์ดแวร์คอมพิวเตอร์ สินค้ารุ่นลิมิเต็ด การดูแลสุขภาพ |
| **การหมุนเวียนที่นั่ง** | การใช้บอทเพื่อเข้ายึดที่นั่งบนเครื่องโดยไม่มีการชำระเงิน ซึ่งมักใช้เวลานานถึง 24 ชั่วโมง | การสูญเสียรายได้จากที่นั่งที่ไม่สามารถขายได้<br><br>ความเสียหายต่อชื่อเสียงเนื่องจากผู้บริโภคที่ถูกต้องไม่สามารถจองเที่ยวบินที่ต้องการได้ | เมื่อใกล้ถึงเวลาออกเดินทางเที่ยวบินที่ดูเหมือนจะถูกจองจนเต็มกลับแสดงจำนวนที่นั่งว่างเพิ่มมากขึ้น | สายการบิน |

# Bad Bot แยกตามอุตสาหกรรม

| อุตสาหกรรม | รวมไปถึงธุรกิจอะไรบ้าง | Bad Bot ทำอะไรได้บ้าง |
|---|---|---|
| **ยานยนต์** | รถเช่า, ผู้ผลิต, ตัวแทนจำหน่าย, ตลาดยานพาหนะ | การดูดข้อมูลราคา การดูดข้อมูล การตรวจสอบสินค้าคงคลัง |
| **บริการทางธุรกิจ** | อสังหาริมทรัพย์ ผู้ขายบุคคลที่สาม เช่น แพลตฟอร์ม การค้าปลีก ระบบ CRM ตัวชี้วัดทางธุรกิจ | การโจมตีที่พุ่งเป้าไปที่ API, การดูดข้อมูล, การเข้าควบคุมบัญชี |
| **คอมพิวเตอร์และไอที** | บริการด้านไอที ผู้ให้บริการด้านไอที ผู้ให้บริการด้านเทคโนโลยี | การเข้าควบคุมบัญชี, การดูดข้อมูล |
| **การศึกษา** | แพลตฟอร์มการเรียนรู้ออนไลน์ โรงเรียน วิทยาลัย มหาวิทยาลัย | การเข้าควบคุมบัญชีสำหรับนักศึกษาและคณาจารย์ ความพร้อมของชั้นเรียน การคัดลอกเอกสารการวิจัยและข้อมูลที่เป็นกรรมสิทธิ์ |
| **บันเทิง** | บริการสตรีมมิ่ง แพลตฟอร์มจำหน่ายตั๋ว บริษัทผู้ผลิต สถานที่จัดงาน | การเข้าควบคุมบัญชี, การดูดข้อมูลราคา, การดูดข้อมูลสินค้าคงคลัง, Scalping |
| **บริการทางการเงิน** | การธนาคาร การประกันภัย การลงทุน Cryptocurrency | การเข้าควบคุมบัญชี Carding การแคร็กการ์ด การดูดข้อมูลเนื้อหาแบบกำหนดเอง |
| **อาหารและร้านของชำ** | บริการจัดส่งอาหาร การซื้อของชำออนไลน์ เว็บไซต์แบรนด์อาหารและเครื่องดื่ม | การฉ้อโกงบัตรเครดิต, การฉ้อโกงบัตรของขวัญ, การเข้าควบคุมบัญชี |
| **การพนัน** | เกมออนไลน์ คาสิโน เดิมพันกีฬา | การเข้าควบคุมบัญชี, การดูดข้อมูลอัตราต่อรอง, การสร้างบัญชีสำหรับการละเมิดการส่งเสริมการขาย |
| **รัฐบาล** | เว็บไซต์กฎหมายและรัฐบาล, บริการพลเมือง, รัฐ, เทศบาล, นครหลวง | การเข้าควบคุมบัญชี, การดูดข้อมูลของรายการจดทะเบียนธุรกิจ, การลงทะเบียนผู้มีสิทธิเลือกตั้ง, การดูดข้อมูลการนัดหมายและกำหนดเวลา |
| **การดูแลสุขภาพ** | บริการด้านสุขภาพ, ร้านขายยา | การเข้าควบคุมบัญชี การดูดข้อมูลเนื้อหา บอท “ที่เป็นประโยชน์” ที่ดูดข้อมูลความพร้อมในการนัดหมาย |
| **ไลฟ์สไตล์** | นิตยสารไลฟ์สไตล์ บล็อก | การดูดข้อมูลเนื้อหาที่เป็นกรรมสิทธิ์ |
| **การตลาด** | เอเจนซี่การตลาด, เอเจนซี่โฆษณา | การดูดข้อมูลเนื้อหาที่เป็นกรรมสิทธิ์ การฉ้อโกงโฆษณา การปฏิเสธการให้บริการ การบิดเบือน |
| **ข่าวสาร** | เว็บไซต์ข่าว นิตยสารออนไลน์ | การดูดข้อมูลเนื้อหาที่เป็นกรรมสิทธิ์ การฉ้อโกงโฆษณา สแปมความคิดเห็น |
| **ร้านค้าปลีก** | อีคอมเมิร์ซ ตลาดกลาง โฆษณาย่อย | การเข้าควบคุมบัญชี, Scalping, การปฏิเสธสินค้าคงคลัง, การฉ้อโกงบัตรเครดิต, การฉ้อโกงบัตรของขวัญ, การดูดข้อมูลและราคา, การบิดเบือนการวิเคราะห์ |
| **ชุมชนและสังคม** | องค์กรที่ไม่แสวงหากำไร, ความศรัทธาและความเชื่อ, ความรักและความสัมพันธ์, ชุมชนออนไลน์, LGBTQ, ลำดับวงศ์ตระกูล | การดูดข้อมูลเนื้อหาและข้อมูล การเข้าควบคุมบัญชี การสร้างบัญชี การทดสอบบัตรเครดิตที่ถูกขโมยในหน้าการบริจาค |
| **กีฬา** | อัปเดตกีฬา ข่าวสาร บริการคะแนนแบบเรียลไทม์ | การดูดข้อมูล (คะแนนสด อัตราต่อรอง ฯลฯ) |
| **โทรคมนาคมและ ISP** | ผู้ให้บริการโทรคมนาคม, Mobile ISP, ผู้ให้บริการโฮสติ้ง | การเข้าควบคุมบัญชี การดูดข้อมูลราคาที่แข่งขันได้ |
| **ท่องเที่ยว** | สายการบิน โรงแรม การจองวันหยุด | การดูดข้อมูลราคาและข้อมูล, การบิดเบือนอัตราส่วน Look-To-Book, การปฏิเสธการให้บริการ, การดูดข้อมูลราคา, การเข้าควบคุมบัญชี, การหมุนเวียนที่นั่ง |

# การวิจัยภัยคุกคามของ Imperva



## สถานะของการรักษาความปลอดภัยของ API ในปี 2024


### การค้นพบที่สำคัญ

71% ของการเข้าชมเว็บทั้งหมดในปัจจุบันเกี่ยวข้องกับ API

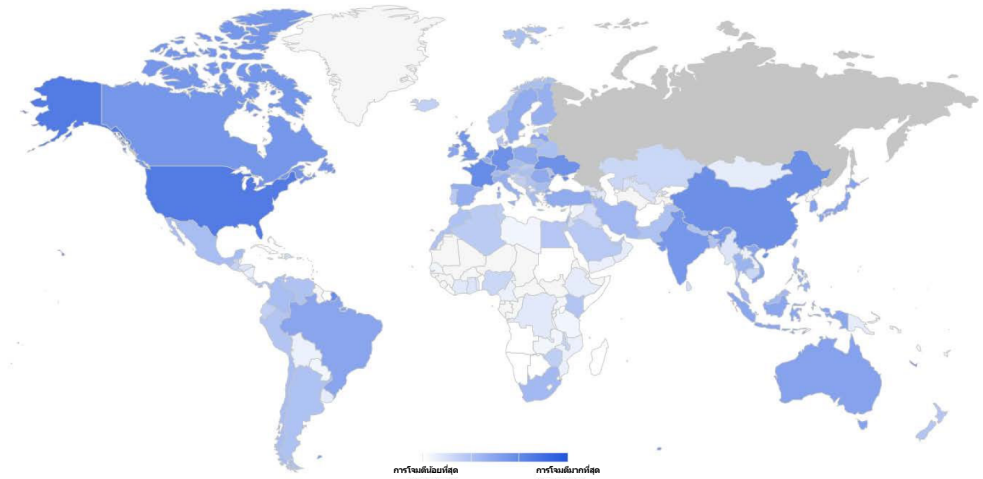
## บทบาทของการป้องกันฝั่งไคลเอ็นต์ในการรักษาความปลอดภัยแอปพลิเคชันสมัยใหม่


### การค้นพบที่สำคัญ

โดยเฉลี่ย เว็บแอปพลิเคชันสมัยใหม่จะโหลดทรัพยากรฝั่งไคลเอ็นต์ 209 รายการตลอดเวลา

## ดัชนีภัยคุกคามทางไซเบอร์

**ดัชนีภัยคุกคามทางไซเบอร์**เป็นการวัดและวิเคราะห์ภาพรวมของภัยคุกคามทางไซเบอร์ทั่วโลกทุก ๆ เดือน ให้คะแนนที่เข้าใจง่ายสำหรับการติดตามระดับภัยคุกคามทางไซเบอร์และสังเกตแนวโน้มอย่างสม่ำเสมอ



# เกี่ยวกับความปลอดภัยของแอปพลิเคชัน Imperva

43

Imperva เป็นผู้นำในการรักษาความปลอดภัยทางไซเบอร์ที่ช่วยให้องค์กรต่าง ๆ สามารถปกป้องแอปพลิเคชัน, API และข้อมูลที่สำคัญได้ทุกที่ ทุกขนาด และได้รับ ROI ในอัตราสูงสุด แพลตฟอร์มการรักษาความปลอดภัยแอปพลิเคชันของ Imperva มีประสิทธิภาพสูงที่สุดในการหยุดยั้งการโจมตี ในขณะเดียวกันก็ลดผลบวกลวงให้เหลือน้อยที่สุด ประสิทธิภาพที่สูงช่วยให้องค์กรต่าง ๆ สามารถเริ่มการดำเนินการได้อย่างรวดเร็วเพื่อปกป้องทรัพย์สินในวงกว้าง ทีมวิจัยภัยคุกคามของ Imperva และชุมชนข่าวกรองทั่วโลกของเราช่วยให้ Imperva มีความก้าวล้ำนำหน้าภูมิทัศน์ภัยคุกคามที่มีวิวัฒนาการอย่างไม่หยุดนิ่งอยู่เสมอ และผสานรวมเอาความเชี่ยวชาญด้านการรักษาความปลอดภัย ความเป็นส่วนตัว และการปฏิบัติตามกฎระเบียบเข้ากับโซลูชันของเราได้อย่างราบรื่น

**แพลตฟอร์มการรักษาความปลอดภัยแอปพลิเคชันของ Imperva เป็นการผสมผสานระหว่างโซลูชันที่ดีที่สุดที่นำเอาการป้องกันในเชิงลึกมาปกป้องแอปพลิเคชันของคุณไม่ว่าจะอยู่บนระบบคลาวด์ ในสถานที่ หรือเป็นแบบค่าแบบไฮบริด:**

- **โซลูชันไฟร์วอลล์เว็บแอปพลิเคชัน (WAF) ภายในองค์กรและบนระบบคลาวด์สำหรับการบล็อกความเสี่ยงต่อความปลอดภัยของแอปพลิเคชันเว็บที่สำคัญที่สุด**
- **การรักษาความปลอดภัยของ API สำหรับการปกป้อง API ทั้งหมดอย่างต่อเนื่องโดยใช้การค้นพบและการจัดหมวดหมู่เชิงลึก**
- **การป้องกันบอทชั้นสูงเพื่อปกป้องเว็บไซต์ แอปพลิเคชันบนอุปกรณ์เคลื่อนที่ และ API จากภัยคุกคามอัตโนมัติที่ซับซ้อนที่สุดในปัจจุบัน**
- **การป้องกันฝั่งไคลเอ็นต์สำหรับการปกป้องเว็บไซต์จากการโจมตีฝั่งไคลเอ็นต์ และปรับปรุงการปฏิบัติตามกฎระเบียบด้วย PCI DSS 4.0**
- **การป้องกัน DDoS สำหรับเว็บไซต์ เครือข่าย และ DNS เพื่อให้มั่นใจถึงความต่อเนื่องทางธุรกิจพร้อมรับประกันความพร้อมใช้งาน**
- **Runtime Application Self-Protection (RASP) เพื่อความปลอดภัยตามค่าเริ่มต้นจากช่องโหว่ที่รู้จักและช่องโหว่ซีโรเดย์**
- **Content Delivery Network ที่นำเสนอแอปพลิเคชันทั่วโลกอย่างปลอดภัยด้วยความเร็วและประสิทธิภาพที่เหนือกว่า**

## เริ่มทดลองใช้การรักษาความปลอดภัยแอปพลิเคชันได้ฟรีวันนี้
## เพื่อปกป้องแอปพลิเคชันของคุณจาก Bad Bot