TOR คืออะไร

The Onion Router (เครือข่ายนิรนาม)

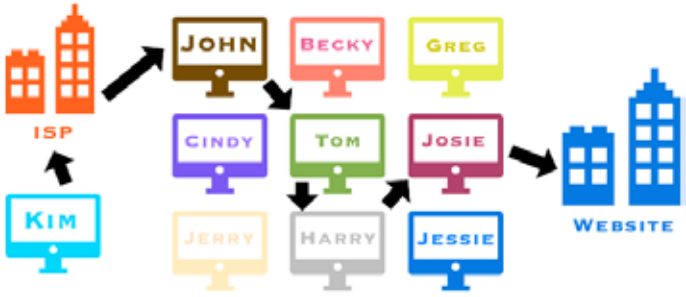
ข้อเท็จจริง

- TOR ย่อมาจาก The Onion Router (เครือข่ายนิรนาม)
- หน่วยปฏิบัติการวิจัยกองทัพเรือ สหรัฐฯ เป็นผู้พัฒนาซอฟต์แวร์ TOR ขึ้นมาเพื่อปกป้องการสื่อสารของหน่วยสืบราชการลับ สหรัฐฯ
- TOR มีจุดมุ่งหมายเพื่อปกปิดตัวตนของผู้ใช้งานและกิจกรรมออนไลน์ของผู้ใช้งานจากการเฝ้าระวังและการวิเคราะห์การรับส่งข้อมูล
- TOR มีการใช้งานที่ถูกต้องตามกฎหมายสำหรับผู้ใช้งานที่ต้องการรักษาความเป็นส่วนตัว หลบเลี่ยงการปิดกั้น หรือปกป้องตนเองจากมาตรการจำกัดสิทธิเสรีภาพหรือการเฝ้าติดตามเป้าหมาย

TOR ทำงานอย่างไร

TOR แปลงข้อมูลที่รับส่งออนไลน์ผ่านเครือข่ายโดยปกปิดตำแหน่งที่ตั้งหรือตัวตนของผู้ใช้งาน แทนที่จะรับส่งข้อมูลอย่างเช่นการเยี่ยมชมเว็บไซต์หรือข้อความโต้ตอบแบบทันทีผ่านเส้นทางแน่นอนที่สามารถคาดเดาได้ [จากผู้ใช้งาน 'Kim' ไปยังเว็บไซต์] TOR จะรับส่งข้อมูลผ่านเส้นทางที่กำหนดที่มีการเปลี่ยนแปลงตลอดเวลาซึ่งทำให้ไม่สามารถตรวจสอบย้อนกลับได้

การเชื่อมต่อ TOR จะถูกเข้ารหัส ลิงก์ที่ไม่ได้เข้ารหัสจะถูกเฝ้าระวัง ทำให้บุคคลอื่นสามารถทราบว่าคุณเยี่ยมชมเว็บไซต์ใดบ้าง โดยตรวจสอบย้อนกลับไปยังที่อยู่ไอพีของคุณ* TOR ใช้การเชื่อมต่อที่เข้ารหัสซึ่งหมายความว่าไม่ว่า ณ จุดใดบนเส้นทางจากผู้ใช้งานอินเทอร์เน็ตต้นทางไปยังตำแหน่งที่ตั้งปลายทาง จะไม่มีความชัดเจนว่าข้อมูลมาจากที่ใดและกำลังจะไปที่ใด



เมื่อ Kim เยี่ยมชมเว็บไซต์ผ่านเครือข่าย TOR การรับส่งข้อมูลของเธอจะใช้เส้นทางแบบสุ่มผ่านคอมพิวเตอร์ของผู้อื่นเพื่อเข้าเว็บไซต์ ที่จุดกึ่งกลางแต่ละจุด ข้อมูลต้นทางและปลายทางจะถูกแยกเป็นส่วนย่อยเพื่อให้ระบุตัวตนของผู้ใช้งานได้ยากมาก ดังนั้น ผู้ให้บริการอินเทอร์เน็ตจึงไม่สามารถตรวจสอบย้อนกลับได้ว่าเธอเป็นใครและกำลังเยี่ยมชมเว็บไซต์ใดอยู่ หรือ TOR จะแสดงโหนดสุดท้าย [Josie] เป็นต้นทางการสื่อสาร

** หมายเลขประจำเครื่องจะแสดงตัวตนของผู้ใช้งานอุปกรณ์ [ดูเอกสารข้อมูล: หมายเลขประจำเครื่องคืออะไร]*

การใช้ TOR ในการล่วงละเมิดทางเพศต่อเด็กและการแสวงหาประโยชน์ทางเพศจากเด็กทางออนไลน์

ผู้ล่วงละเมิดทางเพศต่อเด็กใช้ TOR เพื่อแชร์รูปภาพการล่วงละเมิดทางเพศหรือเนื้อหาอื่นที่เอื้อต่อวัฒนธรรมการล่วงละเมิดทางเพศต่อเด็กและทำให้วัฒนธรรมนั้นคงอยู่ต่อไป นอกจากนี้ TOR ยังช่วยให้ผู้ล่วงละเมิดทางเพศต่อเด็กสามารถเชื่อมต่อกับผู้ที่อาจตกเป็นเหยื่อได้แบบไม่เปิดเผยตัวตน บริการที่มีการปกปิดของ TOR ยังช่วยให้ผู้กระทำความผิดสามารถติดต่อกันเองอย่างลับๆ ได้อีกด้วย ผู้กระทำความผิดหลีกเลี่ยงการเปิดเผยตัวตนหรือตำแหน่งที่ตั้งของตนด้วยการใช้ TOR จึงสามารถหลีกเลี่ยงไม่ให้ผู้ให้บริการอินเทอร์เน็ต (ISP) และหน่วยงานบังคับใช้กฎหมายตรวจพบได้ ดังนั้น TOR จึงทำให้การระบุตัวตนของเหยื่อและผู้กระทำความผิดมีความยุ่งยาก

TOR คือโปรแกรมซอฟต์แวร์ที่เป็นที่นิยมมากที่สุดซึ่งใช้ในการเข้าถึงส่วนต่างๆ ของอินเทอร์เน็ตที่ตั้งใจสร้างขึ้นไม่ให้ใช้งานได้ในวงกว้างหรือไม่ให้สามารถใช้งานได้ง่าย หรือเรียกอีกอย่างว่า "DeepWeb" หรือ "Darknet" (คำหลังหมายถึงลักษณะของการดำเนินการ [ที่ผิดกฎหมาย]) ทั้งนี้ จะสามารถเข้าถึงเครือข่ายคอมพิวเตอร์ที่มีการ 'ปกปิด' มากขึ้นหรือไม่เปิดเผยตัวตนได้โดยใช้ซอฟต์แวร์พิเศษอย่างเช่น TOR

เอกสารข้อมูลนี้จัดทำโดย ECPAT International สนับสนุนการแปลและการผลิตโดย UNICEF