ประจำวันจันทร์ที่ 6 มิถุนายน 2565

FBI ทำการยึดโดเมนที่ใช้ขายข้อมูลที่ถูกขโมยมา และที่ให้บริการโจมตี DDoS

สำนักงานสืบสวนกลางแห่งสหรัฐอเมริกา (FBI) และกระทรวงยุติธรรมสหรัฐแถลงว่าได้มีการยึดโดเมน 3โดเมนที่อาชญากรไซเบอร์ใช้เพื่อขายข้อมูลส่วนบุคคลที่ได้มาจากการละเมิดข้อมูล และการให้บริการโจมตี DDoS

โดเมน WeLeakInfo.to มีการขายข้อมูลเพื่อให้ผู้ใช้งานสามารถเข้ามาค้นหาฐานข้อมูลที่ถูกขโมยมาจากการละเมิด โดยมีมากกว่า 10,000 รายการ โดยมีบันทึกประมาณ 7 พันล้านรายการ ที่เป็นข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ (PII) รวมถึงชื่อ ที่อยู่อีเมล ชื่อผู้ใช้ หมายเลขโทรศัพท์ และรหัสผ่านสำหรับบัญชีออนไลน์ และอีก 2 โดเมน คือ ipstress.in และ ovh-booter.com ถูกใช้เพื่อให้บริการการโจมตีแบบ booter หรือ stressor ซึ่งลูกค้าสามารถขอเว็บไซต์หรือแพลตฟอร์มเว็บที่ตนเลือกเพื่อใช้ในการโจมตี Distributed Denial of Service (DDoS) ทั้งนี้ โดเมนดังกล่าวถูกยึดหลังจากที่มีการดำเนินการบังคับใช้กฎหมายร่วมกันโดยการประสานงานกับกองตำรวจแห่งชาติของเนเธอร์แลนด์ และตำรวจสหพันธรัฐเบลเยียม การดำเนินการบังคับใช้กฎหมายระหว่างประเทศนี้ยังส่งผลให้มีการจับกุมผู้ต้องสงสัย มีการยึดโครงสร้างพื้นฐานของเซิร์ฟเวอร์ และการค้นหาสถานที่ต่างๆ อีกด้วย

ที่มาของข่าว : https://www.bleepingcomputer.com/news/security/fbi-seizes-domains-used-to-sell-stolen-data-ddos-services/