การลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่องบอตเน็ต

(Slowing Down Spam E-mail from Botnet Machines)

วิชิต อาสเสวตร์ , กษิดิศ ชาญเชี่ยว

บทคัดย่อ

ในปัจจุบัน บอตเน็ต (Botnet) ถูกนำมาใช้ในการส่งจดหมายอิเล็กทรอนิกส์สแปม (Spam E-mail) ซึ่งสร้างปัญหากับผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail) งานวิจัยฉบับนี้นำเสนอระบบการลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่องบอตเน็ต Detecting and Slowing Down Spam E-mail System (DSDSE) โดยนำเสนอกระบวนการสำหรับตรวจสอบความผิดปกติของการส่งจดหมายอิเล็กทรอนิกส์ และเทคนิคการตรวจสอบระบบ DNS เพื่อช่วยในการตรวจจับบอตเน็ตที่ส่งจดหมายอิเล็กทรอนิกส์สแปม ผลลัพธ์ที่ได้แสดงให้เห็นว่าระบบ DSDSE สามารถตรวจจับและช่วยลดอัตราการส่งจดหมายอิเล็กทรอนิกส์สแปมจากเครื่องที่เป็นบอตเน็ตได้

ABSTRACT

Currently botnet has been the leading software that spreads spam e-mails, an increasing problem in today's Internet and e-mail usages. This research presents the Detecting and Slowing Down Spam E-mail (DSDSE) system to detect botnet by monitoring DNS traffic and E-mail sending quantity. An algorithm to detect abnormal e-mail sending activities has been proposed. This work also applies a DNS monitoring method to assist detecting botnet machines. The result shows that the DSDSE system can significantly slow down spam e-mail from botnet machines.