CLASSIFICATION OF EXPLOIT-KIT BEHAVIORS VIA MACHINE LEARNING APPROACH

SUKRITTA HARNMETTA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(CYBER SECURITY AND INFORMATION ASSURANCE)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2018

CLASSIFICATION OF EXPLOIT-KIT BEHAVIORS VIA MACHINE LEARNING APPROACH

SUKRITTA HARNMETTA 5837569 ITCY/M

M.Sc. (CYBER SECURITY AND INFORMATION ASSURANCE)

THESIS ADVISORY COMMITTEE: SUDSANGUAN NGAMSURIYAROJ, Ph.D., VASAKA VISOOTTIVISETH, Ph.D.

ABSTRACT

An Exploit Kit (EK) is the cyber-attack tool targeting on finding vulnerabilities appeared on the web browser instances such as web-plugins, or add-on instances installed in a web browser before taking the advantages from the victims' web browser by sending the suitable malware payload through the systems/device/software weak holes they found. This kind of cyber-attack is known as the drive-by download attack in which malware downloading does not require any interaction from users. With sophisticated self-protection mechanism, for example, an EK is capable of imitating a benign website or responding to an end-user with HTTP 404 error whenever they have encountered an unsupported target web browser; this made detecting of EK requires a lot of efforts. However, when an EK launches an attack, there are patterns of interactions between a host and a victim. In this work, we obtained a set of captured traffic from www.malware-traffic-analysis.net and analysed those interactions in order to identify a set of relevant features. Such features were used to build a model for classifying interaction patterns of each EK type. Our experimental results show that with 6,178 network flows and 43 features, our model using the decision tree approach can classify EK traffic and EK type with the accuracy of 97.72% and 96.91%, respectively while the random forest classification model gains 96.60% and 93.27%, and the Naïve Bayes classification model gains 88.97% and 75.85%, respectively. In conclusion, our proposed work can help detect the behaviour of EK with high accuracy.

KEY WORDS: DRIVE-BY-DOWNLOAD / EXPLOIT-KIT / MACHINE LEARNING / NETWORK ANALYSIS / NETWORK SECURITY

95 pages

การแบ่งประเภทพฤติกรรมของ Exploit-Kit โดยใช้วิธีการเรียนรู้ของเครื่อง

CLASSIFICATION OF EXPLOIT-KIT BEHAVIORS VIA MACHINE LEARNING APPROACH

สุกฤตา หาญเมตตา 5837569 ITCY/M

วท.ม.(ความมั่นคงไซเบอร์และการประกันสารสนเทศ)

คณะกรรมการที่ปรึกษาวิทยานิพนธ์: สุดสงวน งามสุริยโรจน์, Ph.D.,วัสกา วิสุทธิวิเศษ, Ph.D.

บทคัดย่อ

Exploit-Kit (EK) คือเครื่องมือที่ใช้โจมตีทางไซเบอร์ซึ่งจะค้นหาช่องโหว่ที่ปรากฏในโปรแกรมเสริมที่ถูกติดตั้งภายในเว็บบราวเซอร์ ตัวอย่างเช่น เว็บปลั๊กอิน และส่วนเสริมต่าง ๆ เป็นต้น ซึ่งอาจจะถูกใช้ส่งมัลแวร์มายังเครื่องปลายทางได้ การโจมตีในรูปแบบนี้รู้จักกันในชื่อการโจมตีแบบ Drive-by-Download ซึ่งเป็นการโจมตีที่ไม่ต้องมีการตอบสนองของผู้ใช้ปลายทาง อีกทั้งยังมีมาตรการการป้องกันตัวเองจากการถูกตรวจพบโดยแอนตี้ไวรัส หรือเมื่อตรวจพบว่าเว็บบราวเซอร์ที่เหยื่อใช้ไม่มีช่องโหว่ที่สามารถโจมตีได้ โดยแสร้งว่าตัวเองเป็นเว็บไซต์ปกติ หรือไม่แสดงหน้าเว็บไซต์ดังกล่าว ดังนั้นการตรวจจับ EK ต้องใช้ความพยายามอย่างสูง อย่างไรก็ตาม มีรูปแบบบางอย่างเกิดขึ้น ณ ขณะที่EKกำลังโจมตี งานวิจัยนี้ใช้ชุดข้อมูลที่ถูกบันทึกไว้ทางเครือข่าย (PCAP file) จากเว็บไซต์ www.malware-traffic-analysis.net มาวิเคราะห์รูปแบบในการโจมตี เพื่อหาคุณลักษณะที่เกี่ยวข้องกับการโจมตีรูปแบบ Drive-by-Downloadโดยใช้EK งานวิจัยนี้ ได้นำคุณลักษณะทางเครือข่ายดังกล่าวมาสร้างเป็นโมเดลที่ใช้การตรวจหา และคัดแยกประเภทของEK ผลการทดลองแสดงให้เห็นว่า จาก6,178การไหลในเครือข่าย และ 45 คุณลักษณะทางเครือข่าย โมเดล Decision Tree สามารถตรวจหาการไหลในเครือข่ายที่ถูกโจมตีด้วย EK ด้วยความแม่นยำ 97.72% และ 96.91% ในการคัดแยกประเภทของ EK ในขณะเดียวกัน โมเดล Random Forest มีความแม่นยำ 96.60% และ 93.27% และโมเดล Naïve Bayes มีความแม่นยำ 88.97% และ 75.85% ตามลำดับ ดังนั้นโดยสรุปคืองานวิจัยนี้ช่วยในการตรวจหารูปแบบการโจมตี Drive-by-Download โดย EK ได้

95 หน้า